



ASIFMA JURISDICTIONAL COMPARISON OF DATA PROTECTION RULES

A comparison of key data protection regulation across APAC jurisdictions

JULY 2020

Developed in kind collaboration with:

Deloitte.

FANGDA PARTNERS
方達律師事務所



HERBERT
SMITH
FREEHILLS

HISWARA
BUNJAMIN &
TANDJUNG



IN ASSOCIATION WITH
HERBERT
SMITH
FREEHILLS



PANAG
& BABU

LAW OFFICES

RAJAH&TANN ASIA

RAJAH&TANN ASIA
LAWYERS
WHO
KNOW
ASIA

	EU / UK	APEC Privacy Framework and the ASEAN Framework	China	India	Hong Kong	Singapore	Malaysia	Thailand	Indonesia	Philippines	Vietnam	Japan	Taiwan	Australia	New Zealand	
Existing	<p>General data privacy and protection rules and regulator</p> <p><i>(General and current laws governing personal data or critical data etc., including requirements for standalone servers and mirroring. Excludes specific rules regarding cloud/virtual data storage which is out of scope)</i></p>	<p>The General Data Protection Regulation (the "GDPR")</p>	<p>The APEC Privacy Framework is available here.</p> <p>The ASEAN Framework on Personal Data Protection is available here.</p>	<p>The Cyber Security Law of the People's Republic of China (the "PRC") (the "CSL") released by the Standing Committee of the National People's Congress and came into force in 2017¹, and its implementation regulations and measures released by various regulators including but not limited to Cyberspace Administration of China and Ministry of Public Security.</p> <p>The General Principles of the Civil Law of the PRC released by the National People's Congress ("NPC") came into force in 2017², which provides a right to personal data protection.</p> <p>The PRC Criminal Law released by the NPC came into force in 2017³, criminalizing the intrusion of information systems and other cybercrimes, which have been relied upon in prosecuting personal data protection infringements.</p> <p>The Decision on Strengthening the Protection of Online Information released by the Standing Committee of the NPC came into force in 2012⁴, which provides certain general principles on the protection of citizen's online information.</p> <p>The Measures on the Protection of Personal Data of Telecommunication and Internet Users released by the Ministry of Industry and Information Technology (the "MIIT") came into force in 2013⁵, which provide relevant rules on the protection of users' personal data.</p> <p>The Administrative Measures for the Multiple Level Protection System of Information Security collectively released by (i) the Ministry of Public Security, (ii) National Administration of State Secrets Protection, (iii) the State Cryptography Administration Bureau, and (iv) the Information Office of the State Council came into force in 2007⁶, providing relevant rules for Multiple Level Protection System (these measures are generally referred to as "MLPS 1.0").</p> <p>In addition to above-mentioned laws and regulations, there are various national standards on privacy and data protection in China i.e. the recommended national standards the Information Security Technology-Personal Information Security Specification (the "Personal Information National Standard") released by the National Information Security Standardization Technical Committee in 2017. Please note that after going through several rounds of revision since the end of 2018, the second edition of the Personal Information National Standard⁷ was released on 6 March 2020 and will be effective from 1 October 2020.</p>	<p>Currently, the regulations relating to personal data protection in India are contained in the Information Technology Act 2000 (as amended) ("IT Act"); and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 was issued thereunder ("SPDI Rules").</p> <p>At present, there is no designated authority for data privacy matters; however, contraventions of the IT Act and rules made thereunder dealt with by adjudicating officers, and the cyber appellate tribunal constituted under the IT Act.</p> <p>The PDP Bill (see Row 3 below) would establish a Data Protection Authority (the "DPA").</p>	<p>Personal Data (Privacy) Ordinance (Cap. 486) (the "PDPO"). and supplementary regulations issued thereunder.</p> <p>The PDPO is administered and enforced by the Office of the Privacy Commissioner for Personal Data (the "Commissioner")</p> <p>The Commissioner also issued a number of codes of practice and guidelines.</p>	<p>The Personal Data Protection Act 2012 (the "PDPA") and supplementary regulations issued thereunder.</p> <p>The PDPA is administered and enforced by the Personal Data Protection Commission ("PDPC").</p> <p>The PDPC also issued a number of advisory guidelines.</p>	<p>The Personal Data Protection Act (the "PDPA") and related subsidiary legislation issued thereunder.</p> <p>The PDPA is administered and enforced by the Office of Personal Data Protection Commissioner (the "Commissioner").</p> <p>The Commissioner also issued a number of codes of practice and FAQs.</p>	<p>The Personal Data Protection Act (the "PDPA") and supplementary regulations issued thereunder.</p> <p>The PDPA is administered and enforced by the Personal Data Protection Commission ("PDPC"); and the Office of Personal Data Protection Commission ("PDPC's Office"), a government agency to promote and support the development of personal data protection.</p> <p>Provisions under Chapters 2, 3, 5, 6, 7, Sections 95, and Section 96 of the PDPA will become effective on 27 May 2020.</p>	<p>There is no general law on personal data protection. The key regulations which apply to general personal data privacy are as follows:</p> <ol style="list-style-type: none"> 1. Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016 ("EIT Law"); 2. Government Regulation No. 71 of 2019 on Administration of Electronic System and Transaction ("GR 71"); and 3. Minister of Communication and Informatics Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems ("Regulation 20") <p>In addition to the above regulations, sectoral legislation may apply.</p>	<p>The privacy and data protection in the Philippines is governed by the Data Privacy Act of 2012 (DPA) or Republic Act 10173, which provides comprehensive protections for personal information. It is supported by the Implementing Rules and Regulations of the Data Privacy Act of 2012.</p> <p>The National Privacy Commission is the independent body tasked to administer and implement the provisions of the Act.</p> <p>In comparison to its neighbours, the Philippines has one of the stronger privacy regimes in the Asia Pacific region. With a rapidly growing IT, digital economy, and social media users, the Government and privacy regulator has a mandate to protect the privacy of individuals and ensure the free flow of information.</p>	<p>Vietnam does not have a comprehensive legislative regime or regulatory body responsible for privacy. There are varied requirements relating to the protection of personal information across a number of laws.</p> <p>The Law on Network Information Security (86/2015/QH13) ("NIS Law"), also widely referenced as the Law on Cybersecurity, establishes the most comprehensive requirements and definitions regarding the protection of personal information. These requirements apply to individuals and organizations engaged in information technology application and development activities.</p> <p>There are a number of laws and regulations that apply to certain sectors and types of transactions, such as the Law on Protection of Consumers' Rights, the Law on Information Technology and the Decree on E-Commerce, which may apply to personal information.</p> <p>Primary legislation: Law on Network Information Security (86/2015/QH13) ("NIS Law")</p>	<p>Personal Information Protection Act (PIPA) Japanese amended law was fully effective as of 30 May 2017. In Japan, privacy is regulated by the Act on the Protection of Personal Information ("APPI").</p> <p>The APPI is a comprehensive privacy law administered by the Personal Information Protection Commission ("PPC"); it applies to personal information handling business operators ("PIHBO") to protect the interests of principals. The PPC issued an interim draft report, which revealed plans for Japan to revise its existing personal information protection law in 2020. The focus will be to introduce a right to be forgotten, which would be applied cross Japan's borders.</p>	<p>In Taiwan, personal information is protected under the Personal Information Protection Act (PIPA) (sometimes referred to as PDPA), which is enforced by industry regulators and local government authorities.</p> <p>The legislation was enacted in 1995 and amended in 2010 and 2015. When drafted, the PIPA considered the European Data Protection Directive (Directive 95/46/EC). In 2018, Taiwan was admitted to the Asia-Pacific Economic Forum's Cross Border Privacy Rules system, which aims to 'build consumer, business, and regulator trust in cross border flows of personal information', making it only the 7th APEC country to do so, highlighting an increased focus on privacy.</p>	<p>The general national privacy law in Australia is the Privacy Act 1988, supported by other legislation such as the Privacy Regulation 2013, the Spam Act 2003 and various state acts that deal with sectoral privacy, such as privacy in the workplace and health information privacy.</p> <p>The national privacy regulator is the Office of the Australian Information Commissioner.</p>	<p>The Privacy Act 1993 controls how 'agencies' collect, use, disclose, store, and give access to personal information.</p> <p>Regulator: The Office of the New Zealand Privacy Commissioner was established to administer the Privacy Act 1993. The Privacy Commissioner is entrusted to protect personal information of New Zealanders in accordance with the Privacy Act.</p>

¹ The Chinese text of the CSL is available at http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm

² The Chinese text of the General Principles of the Civil Law of the PRC is available at http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-03/15/content_2018907.htm.

³ The Chinese text of the PRC Criminal law amended in 1997 is available at http://www.npc.gov.cn/wxzl/wxzl/2000-12/17/content_4680.htm, and the Chinese text of the Amendments XII and IX which criminalized the intrusion of information systems and other cybercrimes is available at http://www.npc.gov.cn/wxzl/gongbao/2009-06/09/content_1517170.htm and http://www.npc.gov.cn/zgrdw/npc/xinwen/2015-08/31/content_1945440.htm respectively.

⁴ The Chinese text of the decision is available at http://www.npc.gov.cn/wxzl/gongbao/2013-04/16/content_1811077.htm

⁵ The Chinese text of the measures is available at <http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057729/c4700145/content.html>.

⁶ The Chinese text of the administrative measures is available at http://www.gov.cn/jzdt/2007-07/24/content_694380.htm.

⁷ The Chinese text of the national standard is available at <http://c.gb688.cn/bzgk/gb/showGb?type=online&hcno=4568F276E0F8346E0FBA097AA0CE05E>.

<p>2. Additional rules for financial services (Confidentiality, Information Security, Bank Secrecy, including relating to intercompany third-party transfers)</p> <p>(Any additional regulation on collection, processing, or transfers of personal or critical data etc. applicable to regulated financial services or payments / applicable to financial institutions only.)</p>	<p>N/A</p>	<p>N/A</p>	<p>China Banking and Insurance Regulatory Commission (the "CBIRC"), China Securities Regulatory Commission (the "CSRC"), and the People's Bank of China (the "PBOC") are the sectoral regulators for the financial services industry. Each of these sectoral regulators have issued certain sectoral rules that cover cybersecurity and data protection, including but not limited to the following:</p> <ul style="list-style-type: none"> • The Personal Financial Information Protection Technical Specification that was released by the PBOC on 13 February 2020. • The Administrative Measures on Anti-money Laundering and Counter-terrorist Financing by the Banking Financial Institutions that was issued by CBIRC 19 January 2019. • The Guidelines on Data Governance of Banking Financial Institutions that was issued by the CBIRC on 21 May 2018. • The Implementing Measures for the Protection of Rights and Interests of Financial Consumers that was issued by the PBOC on 14 December 2016. • The Guidelines on Protection of Rights and Interests of Banking Consumers that was issued by the CBRC (now CBIRC) on 30 August 2013. • The Circular on Emphasis to Banking Financial Institutions on Protecting Personal Financial Information that was issued by the PBOC on 21 January 2011. • The Provisional Rules on Management of the Individual Credit Information Database that was issued by the PBOC on 18 August 2005. <p>In 2011, PBOC Notice to Urge Banking Financial Institutions to Protect Personal Information, Article 3.6</p> <ul style="list-style-type: none"> • Requesting domestic storage and processing • Personal financial information (PI) of Chinese citizens collected in PRC shall be stored, processed and analyzed in PRC. <p>In 2019, CBIRC Banking Financial Institutions Anti-money Laundering and Counter Terrorist Financing Management Measures (CBIRC 2019 Decree No. 1), Article 28</p> <ul style="list-style-type: none"> • Prohibiting cross-border transfer of client identification and transaction info collected during AML/CTF process 	<p>RBI has recognized that a banker's "obligation to maintain secrecy" arises out of the contractual relationship between the banker and client, whereby no information should be divulged to third parties".</p> <p>While there continues to be divided interpretations on whether the term "under compulsion of law" encompasses only Indian law or also include foreign law, considering that the RBI has not limited the definition by specifying that the disclosure would be as per Indian laws, it may be interpreted to include disclosures mandated by foreign law.</p>	<p>The Hong Kong Monetary Authority has issued a Circular on Customer Data Protection and a Supervisory Policy Manual on Risk Management of E-banking which contain provisions that are relevant to data protection.</p> <p>Other regulators (such as the Securities and Futures Commission) and industry associations (such as the Insurance Authority) have respectively published guidelines covering outsourcing, which also contain relevant provisions relating to data protection. For example, the SFC has recently issued a Circular to Licensed Corporations on the use of external electronic data storage providers.</p> <p>The SFC also issue circulars from time to time in response to specific threats.</p>	<p>Section 47 of the Banking Act ("BA") sets out the banking secrecy and confidentiality obligations. Section 47 of the BA prohibits bank/bank officers in Singapore from disclosing customer information to any other person (except as expressly provided in the BA). Disclosure of customer information may be allowed for the purpose of outsourcing of the bank's operational functions among other available exceptions.</p> <p>In relation to governance, systems, and controls, the Monetary Authority of Singapore ("MAS") has issued the Technology Risk Management Guidelines ("TRM Guidelines") published in 2013.</p> <p>Other guidelines issued by the MAS for financial institutions to mitigate cybersecurity risks, include the Outsourcing Guidelines and Business Continuity Management Guidelines ("BCM Guidelines").</p> <p>A licensee under the Payment Services Act must comply with the cyber hygiene requirements as set out in the MAS Notice on Cyber Hygiene and put in place appropriate safeguards to protect customer information. A licensee should also understand and apply the relevant MAS Guidelines such as the TRM Guidelines and E-payments User Protection Guidelines.</p>	<p>The Personal Data Protection Code of Practice for the Banking and Financial Sector issued by the Commissioner.</p> <p>Banking secrecy provisions are stipulated in the Financial Services Act 2013 ("FSA") and the Islamic Financial Services Act 2013 ("IFSA"), which prohibit financial institutions and officers of a financial institution from disclosing customer information to any person, except as expressly provided in the FSA and IFSA.</p> <p>The Central Bank of Malaysia (Bank Negara Malaysia or "BNM") has issued several guidelines and policy documents in respect to the management of customer information, which include (but are not limited to): (a) Policy Document on Management of Customer Information and Permitted Disclosures; (b) Policy Document on Outsourcing; (c) Guidelines on Data Management and MIS Framework; (d) Policy Document on Risk Management in Technology ("RMIT").</p>	<p>The Bank of Thailand (the 'BOT') has issued the BOT Regulation pursuant to the Financial Institution Act 2008. This includes a Know Your Customer (KYC) guideline for deposit taking financial institutions, which requires them to set up an appropriate Data Governance Policy and Data Classification Policy that covers every process of data usage including the method to collect, access, transfer, and destroy customer personal data in order to ensure that such data is secured.</p> <p>The BOT has also issued a guideline on Information Technology Risk.</p> <p>For payment system providers, BOT has issued regulation no.4/2018 under the Payment System Act 2017. This governs personal data protection of the payment system user by the payment system provider. Note that the PDPA supersedes this Act with respect to collection, use, or disclosure of personal data.</p>	<p>Key rules for the financial services sector include:</p> <p>Banking Secrecy Rules:</p> <ol style="list-style-type: none"> 1. Law No. 7 of 1992 on Banking as amended by Law No. 10 of 1998 2. Regulation of Bank Indonesia ("BI") No. 2/19/PBI/2000 on Requirements and Procedure on the Granting of Order or Written Approval to Disclose Banking Secrecy <p>BI Transparency Rules:</p> <p>Regulation of BI No. 7/6/PBI/2005 and Circular of BI No. 7/25/DPNP- both on Transparency of Banking Products Information and the Use of Customer Personal Data</p> <p>Indonesia Financial Authority (Otoritas Jasa Keuangan – "OJK") Customer Protection Rules:</p> <ol style="list-style-type: none"> 1. Regulation of OJK No. 1/POJK.07/2013 on Customer Protection in the Financial Services Sector (as partly revoked by Regulation of OJK No. 76/POJK.07/2016 and Regulation of OJK No. 18/POJK.07/2018) 2. Circular of OJK No. 14/SEOJK.07/2014 on Confidentiality and Security of Customer Personal Information and/or Data 3. Regulation of OJK No. 38/POJK.03/2016 on the implementation of risk management in the use of information technology by commercial banks as amended by Regulation of OJK No. 13/POJK.03/2020 <p>Others:</p> <p>Regulation of BI No. 18/40/PBI/2016 on Payment Transaction Processing Operators and Regulation of BI No. 14/23/PBI/2012 on Fund Transfer, as implemented by:</p> <ol style="list-style-type: none"> a. Circular of BI No. 18/41/DKSP on Payment Processing Implementation b. Circular of BI No. 15/23/DASP on Fund Transfer as partly revoked by Circular of BI No. 16/1/DKSP on Fund Transfer Reporting 	<p>Republic Act 1405 is the law that prohibits the disclosure or inquiry into deposits with any banking institution. All deposits of whatever nature with banks or banking institutions in the Philippines including investments in bonds issued by the Government of the Philippines, its political subdivisions and its instrumentalities, are hereby considered as an absolutely confidential nature and may not be examined, inquired or looked into by any person, government official, bureau or office, except upon written permission of the depositor, or in cases of impeachment, or upon order of a competent court in cases of bribery or dereliction of duty of public officials, or in cases where the money deposited or invested is the subject matter of the litigation.</p> <p>Banko Sentral ng Pilipinas (BSP) issued Circular 982 "Enhance Guidelines on Information Security Management" to strengthen cyber security polices among the financial organizations. According to the Circular, all supervised financial institutions should establish robust and effective technical security risk management processes, governance and cybersecurity controls to prevent compromise of their financial stability; to ensure operational resilience; and to protect the data of the consumers.</p> <p>In Circular 982, Section 2.6, it states that in designing the Information Security Program, financial institutions must consider relevant laws and regulations including the Philippines Data Privacy Act of 2012 to support the data privacy requirements.</p>	<p>The government of Vietnam issued Decree No. 117/2018/ND-CP on confidentiality and disclosure of customer information of credit institutions and branches of foreign banks (Decree 117). Decree 117 took effect on November 1, 2018, replacing Decree No. 70/2000/ND-CP of 2000 on confidentiality, storage, and disclosure of information related to customer deposits (Decree 70).</p>	<p>Multiple Privacy guidelines are published by PPC. Data protection is included in FISC guideline for financial industry.</p> <p>FISC: https://www.fisc.or.jp/eng/lish/ additional rule is available for international data transfer from EU, based on GDPR adequacy decision.</p>	<p>Financial sectors are required to comply with Financial Supervisory Commission (FSC) "Measures for the Security Maintenance of Personal Data of Non-Public Organizations" (非公務機關個人資料檔案安全維護辦法) whereas detail privacy security requirements.</p> <p>If the process of PI concerns with third party or cloud, it also needs to comply with "Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation".</p>	<p>There are broad confidentiality and information security laws that apply to the banking sector in Australia, which extends to the protection of personal information. These obligations have their origin in legislation & common law and equity. There are also obligations that need to be followed under industry codes (such as the Code of Banking Practice) and regulator guidelines (such as APRA's CPS 234).</p> <p>APRA's CPS 234 has provisions that need to be complied from a third-party transfer perspective, in addition to the general rules that the banking industry must comply with under the Privacy Act 1988.</p>	<p>No information found that is released by the Reserve Bank of New Zealand (RBNZ) and the New Zealand Financial Markets Authority (FMA).</p> <p>Most banks refer to the Australian standards such as APRA CPS 234: Information Security Prudential Standard.</p> <p>The Privacy Act 1993 gives the Privacy Commissioner power to issue codes of practice that become part of the law. These codes may modify the operation of the Act for specific industries, agencies, activities, or types of personal information. Codes often modify one or more of the information privacy principles to take account of special circumstances, which affect a class of agencies (e.g. credit reporters) or a class of information (e.g. health information).</p> <p>Credit Reporting Privacy Code 2004 applies specific rules to credit reporters to better ensure the protection of individual privacy. The code addresses the credit information collected, held, used, and disclosed by credit reporters. For credit reporters, the code takes the place of the information privacy principles.</p> <p>Superannuation Schemes Unique Identifier Code 1995 provide agencies involved with certain superannuation schemes with a potential exemption from information privacy principle 12(2) when those agencies reassign a unique identifier for clients.</p> <p>New Zealand Bankers Association (NZBA) is a non-profit, unincorporated organisation funded by member banks through subscriptions. Full membership of the Association is open to any bank registered under the Reserve Bank of New Zealand Act 1989. Industry body commitment to respect customers, including privacy and information security. Generally, the code specifies:</p> <ul style="list-style-type: none"> - When you deal with us, we will do these things. - Treat you fairly and reasonably. - Communicate with you clearly and effectively. - Respect your privacy and confidentiality and keep our banking systems secure. - Act responsibly if we offer or provide you with credit. - Deal effectively with your concerns and complaints. <p>Also sets out guidelines to help banks meet the needs of older and disabled customers.</p>
--	------------	------------	---	--	---	---	---	--	--	---	--	--	---	--	---

	EU / UK	APEC Privacy Framework and the ASEAN Framework	China	India	Hong Kong	Singapore	Malaysia	Thailand	Indonesia	Philippines	Vietnam	Japan	Taiwan	Australia	New Zealand
New	<p>Proposed new data privacy and protection rules</p> <p>No amendments to the GDPR are currently proposed. However, the EU's ePrivacy Directive (governing, amongst other things, the use of cookies and electronic marketing) is currently being revised. The revised ePrivacy Regulation was due in 2018 but has still not been agreed. It is now unlikely to be in force before 2023, with a two year implementation period to 2025.</p> <p>In addition, the legislative landscape in the UK could be subject to change following the expiration of the Brexit 'transition period' at the end of December 2020.</p> <p>A controller does not have to notify a regulator or data subjects of a data breach if the breach is unlikely to result in a risk to the rights and freedoms of natural persons.</p>	<p>No plan to revise privacy rules but growing consensus around need to revise APEC cross border privacy rules system, given lack of take up and inaccessibility for banks and SMEs, among others.</p>	<p>Since the passage of the CSL in 2016, the Cyberspace Administration of China (the "CAC") has been making various rules to implement the CSL. The CAC released various draft rules in 2019 on cybersecurity and data protection, such as:</p> <ul style="list-style-type: none"> • The draft of Measures for the Administration of Publishing Cyber Threat Information that was released on 20 November 2019 for public consultation. • The draft Measures on Security Assessment on Cross-border Transfer of Personal Data was released on 13 June 2019 for public consultation. • The draft of Regulations on Administration of Data Security was released on 28 May 2019 for public consultation. These draft regulations specify the rules on the protection of personal data and important data under the CSL. • The finalized version of the Measures for Cybersecurity Assessment was released on 13 April 2020 and will come into force on 1 June 2020. These measures are made to implement Article 35 of the CSL, which requires that any purchase of network products and services by the critical information infrastructure (the "CII") operators (the "CIO") that affects or may affect state security is subject to relevant cybersecurity assessment. <p>Recent ASIFMA/GFMA submissions to these consultations are set out below:</p> <p>1) 12 July 2019, Draft of the Measures on Security Assessment on Cross-border Transfer of Personal Data – LINK</p> <p>2) 24 June 2019, Draft of the Measures on Administration of Data Security – LINK</p> <p>The Ministry of Industry and Information Technology (the "MIIT") has also released certain draft rules in 2019 for the implementation of certain articles under the CSL, such as:</p> <ul style="list-style-type: none"> • The draft Measures for the Administration of Cybersecurity Vulnerabilities was released on 18 June 2019. • The draft of Implementing Measures for the Security Detection of Critical Network Equipment was released on 4 June 2019. <p>The national standard for MLPS 2.0, which comprises of various national standards that have been revamped, has been jointly released by the State Administration of Market Regulation and the Standardization Administration of China earlier in June 2019.</p>	<p>Personal Data Protection Bill (PDPB) 2019 (Published 3 Feb 2020)</p> <p>On 27 July 2018, a committee of experts led by Justice Srikrishna presented their report- along with draft data protection legislation- titled the 'Personal Data Protection Bill, 2018' to the Ministry of Electronics and Information Technology ("MEITY").</p> <p>Thereafter, on 10 December 2019, a revised copy of the (draft) Personal Data Protection Act, 2019 ("PDP Bill") was circulated to certain stakeholders such as Members of Parliament. It is unclear as to when the PDP Bill will be tabled in Parliament.</p> <p>The Joint Parliamentary Committee ("JPC") on 3 Feb 2020 launched a three weeks long consultation on the PDP Bill. The JPC also signalled an option of in-person meeting. Earlier, the JPC was granted time until the end of the budget session (typically held between February and May) to table its report.</p> <p>Issues with the PDP Bill are set out where relevant in the rest of this table.</p> <p>Data fiduciaries are required to notify the DPA as soon as possible and within such timelines, as specified by the DPA of personal data breaches likely to cause harm to data principals. Such reportings should include details of the nature of data breach, number of affected data principals, possible consequences and remedial measures. Presumably, those data breaches which do not cause "harm" to data principals need not be reported. Under the PDP, the term "significant harm" is defined as "significant harm" that has an aggravated effect, having regard to the nature of the personal data being processed, the impact, continuity, persistence, or irreversibility of the harm.</p>	<p>Yes – on 13 January 2020, a consultation paper was issued by the Constitutional and Mainland Affairs Bureau along with Commissioner suggesting potential areas of reform to the PDPO ("Consultation Paper"), which recommended:</p> <p>(i) the introduction of a mandatory data breach notification mechanism; (ii) raising the sanctioning powers of the Commissioner to directly impose administrative fines for the contravention of the PDPO; (iii) the PDPO be amended requiring data users to formulate a clear retention policy, specifying a retention period for the personal data collected; (iv) amending the definition of personal data; and (v) that the PDPO should be amended so that data processors are directly accountable for personal data retention and security, and render them responsible for data breach notifications upon becoming aware of any data breach incidents</p> <p>There was no indication in the Consultation Paper of an express timeframe for the completion of the review process or when specific amendments to the PDPO would be proposed.</p>	<p>PDPC consulted in 2017 on a mandatory data breach notification regime and the introduction of "legitimate interest" as a basis to collect, use, or disclose personal data regardless of consent.</p> <p>PDPC's Guide to Managing Data Breaches 2.0 dated 22 May 2019 provides (non-mandatory) guidelines as to when an organisation is required to notify the PDPC and/or affected individuals about a data breach. These guidelines will likely form the framework that will be introduced by the PDPC as part of the mandatory data breach notification regime. These are broadly similar to GDPR provisions.</p> <p>The PDPC has indicated its intention to introduce a data portability requirement in Singapore.</p> <p>Under the PDPC's Guide to Managing Data Breaches 2.0, an organisation needs to notify PDPC when the data breach is:</p> <ul style="list-style-type: none"> • likely to result in significant harm or impact to the individuals to whom the information relates; or • of a significant scale (i.e. a data breach involves personal data of 500 or more individuals). <p>An organisation needs to notify affected individuals (including parents and the legal guardians of minors whose personal data is affected) when the data breach is likely to result in significant harm or impact to the individuals to whom the information relates.</p> <p>As such, it follows that potential exemptions for breach notification exist where personal data is subjected to encryption or anonymisation such that the breach is not likely to result in significant harm or impact to the individuals.</p>	<p>In February 2020, the Commissioner issued the Public Consultation Paper No.1/2020 on Review of the Personal Data Protection Act 2010, which proposed wide ranging reforms to the PDPA, including:</p> <ul style="list-style-type: none"> • The imposition of direct obligations on data processors to comply with the PDPA; • Introduction of new rights and concepts in the PDPA, such as the right to data portability and the concept of privacy by design; • Requirement for data users to appoint a data protection officer; • Introduction of a mandatory data breach notification regime; • Removal of the "whitelisted" provisions in the PDPA for transfers of personal data outside of Malaysia; • Establishment of a Do Not Call Registry in Malaysia; • New provisions to provide for the data subjects' right to bring civil claims against the data user for breach of the PDPA; • Extending the application of the PDPA to the Federal and State Governments, as well as to non-commercial activities; • Exemption of business contact information from the ambit of the PDPA; • Extra-territorial application of the PDPA in respect of persons who monitor the behavior of Malaysian data subjects, etc. <p>The public consultation period ended in March 2020 but it remains to be seen when the proposed reforms will be officially tabled in Parliament.</p>	<p>Provisions under Chapters 2, 3, 5, 6, 7 and Sections 95 and Section 96 of the PDPA will become effective on 27 May 2020.</p> <p>Pursuant to section 37 (4), the data breach notification would not be required if such breach has no risk of impact to the right and freedom of any person. In addition, the exemption of data breach notification will be set out in the PDPC's notification (nothing further actually prescribed).</p>	<p>The following new pieces of legislation are anticipated in Indonesia. The timing for the introduction of each additional law remains unknown.</p> <p>1. Law on Personal Data Protection – this will be general framework on personal data protection (the "Personal Data Protection Law")</p> <p>The draft Personal Data Protection Law is intended to be an umbrella legislation for personal data protection in Indonesia. Currently, personal data protection in Indonesia is piecemeal, being set out in several regulations. Much of the draft Personal Data Protection Law draws on concepts in the European Union's General Data Protection Regulation ("GDPR"). The draft Personal Data Protection Law includes, among others, (1) concepts of data controllers and data processors (2) concept of sensitive personal data and (3) other legal basis for data processing, mainly inspired by the GDPR, but also includes other concepts unique to Indonesia, such as the concept of personal data "owners" (rather than data "subjects") and imposing criminal sanctions for certain data breaches. The draft Personal Data Protection Law also prohibits the sale of personal data.</p> <p>Breach notification: A data controller must submit written notification within 3x24 hours to: (i) the relevant personal data owner; and (ii) MOCI if there is any failure to personal data protection.</p> <p>This obligation would be exempted for the purpose of: (i) national defence and security interests, (ii) legal enforcement interests, (iii) public interests in the context of state administration, (iv) supervisory interests for the financial, monetary, payment system and financial system's stability, or (v) data aggregation for the purpose of statistical and scientific research in state administration.</p>	<p>There are two pending bills to amend the DPA: http://congress.gov.ph/legis/docs/basic_18/HB05612.pdf and http://congress.gov.ph/legis/docs/basic_18/HB01188.pdf</p> <p>Public consultations are currently being conducted, and the local finance sector is actively participating. (Dondi from Citigroup pointed out that these are taking place)</p> <p>Exemptions for breach notification: Notification is not required if the National Privacy Commission determines: 1. that notification is unwarranted after taking into account compliance by the Personal Information Controller with the Act and the existence of good faith in the acquisition of personal information, or 2. in the reasonable judgment of the National Privacy Commission, such notification would not be in the public interest or in the interests of the affected data subjects.</p>	<p>None</p>	<p>PIPA will be amended in 2020. (It is amended every 3 years in accordance with Law definition.)</p> <p>Exemptions for breach notification: It is not legally required to report a data breach incident to the PPC or to notify the relevant data subjects. With reference to PPC guidelines, if a factual situation demonstrates that the Personal Data, which has been disclosed, was immediately collected before being seen by any third party or not actually disclosed, the notice to the PPC or any other relevant authority is not necessary. An example is that the company has encrypted the data or otherwise secured the data in such a way that it has become useless to third parties being in possession of such data.</p>	<p>There is no concrete proposal for amendments to the current Data Privacy Act of the Philippines.</p> <p>Exemptions for breach notification: There are no general exemptions for breach notification as in general where personal data is stolen, disclosed, altered, or infringed in other ways due to the violation of the PDPL, the data controller should notify the data subject after due inquiry.</p>	<p>There are currently no proposed new laws for privacy in Australia; however, the Australian Competition and Consumer Commission released their Digital Platforms Inquiry Report in 2019, which highlighted several areas that need strengthening in Australian privacy law- most notably around rights and consent. In response, the Australian Government indicated that these recommendations will be further examined in 2020 to support any policy proposal for privacy law uplift.</p>	<p>New Zealand Government is currently in the process of making changes to the Privacy Act. The Minister of Justice introduced a Bill amending the current Act on 20 March 2018, which is anticipated to be passed in 2020.</p>

	EU / UK	APEC Privacy Framework and the ASEAN Framework	China	India	Hong Kong	Singapore	Malaysia	Thailand	Indonesia	Philippines	Vietnam	Japan	Taiwan	Australia	New Zealand
4.	Proposed new financial services sector rule <i>(e.g. Confidentiality, Information Security, Bank Secrecy, including relating to intercompany third-party transfers)</i>	None	N/A	<p>• As reported, the PBOC recently prepared a draft of the Interim Measures for the Protection of Personal Financial Information, which provided draft measures to certain Chinese financial institutions in October 2019 for consultation. These draft measures may apply to the collection, processing, use, and disclosure of personal financial data by various financial institutions in China. These measures, when finalized, may consolidate the requirements on protecting personal financial data of banking individual customers that are scattered in various rules.</p> <p>• The PBOC released a new draft of the Implementation Measures for the Protection of Rights and Interests of Financial Consumers on December 27 2019 (the "Draft Implementation Measures"). The Draft Implementation Measures aim to replace (i) the Implementation Measures for the Protection of Rights and Interests of Financial Consumers that were issued by the PBOC and came into force on 14 December 2016 and (ii) the Administrative Measures for the Protection of Rights of Financial Consumers (Trial) that were issued by the PBOC and came into force on 7 May 2013. The Draft Implementation Measures reiterate data storage and processing localization requirement as well as other protection obligations of financial institutions in terms of their processing of consumer financial information.</p>	None	None	None	None	None as at the date of this summary table	None	None	N/A	No concrete proposal for additional data privacy and protection rule.	None	<p>No information found that is released by the Reserve Bank of New Zealand (RBNZ) and the New Zealand Financial Markets Authority (FMA).</p> <p>Changes to the Credit Reporting Privacy Code (Amendment No 14) were made in three stages in 2019, following a 18-month review into the operation of the comprehensive credit reporting system. The changes were intended to make the credit reporting system fairer for consumers and improve enforcement and compliance.</p> <p>Amendment No. 14 changes came into force in three phases on 1 July, 1 April, and 1 October 2019. The latest changes increase the threshold for listing overdue payments as defaults in credit reports. It also obliges credit providers to issue quotation enquiries when offering risk-based pricing for credit products.</p> <p>Superannuation Schemes Unique Identifier Code 1995 Amendment No. 1. The Code has been amended by Amendment No. 1 and commenced on 15 October 2015. Amendment No 1 will make two minor changes to the Code. Firstly, it will amend the definition of the term "associated person" to replace a reference to section OD7 of the Income Tax Act 1994 (which has since been repealed) with its current equivalent – subpart YB of the Income Tax Act 2007. Secondly, it will remove clause 3(2). This subsection sets out that terms and expressions used in the Code but which are defined in the Privacy Act 1993 or Acts Interpretation Act 1924 (which has since been replaced by the Interpretation Act 1999) have the same meanings respectively as in those Acts.</p>

	EU / UK	APEC Privacy Framework and the ASEAN Framework	China	India	Hong Kong	Singapore	Malaysia	Thailand	Indonesia	Philippines	Vietnam	Japan	Taiwan	Australia	New Zealand
5. Definitions	<p>Definition of 'Personal' data (or similar), and extraterritorial application/exclusions related to such definitions</p> <p>Definition of Personal Data Under Article 4 of the GDPR, "personal data" means any information relating to an identified or identifiable natural person (the "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</p> <p>Extra-territorial Application Under Article 3 of the GDPR, the GDPR applies to:</p> <ul style="list-style-type: none"> the processing of personal data in the context of the activities of a controller or processor; or the processing of personal data of a data subject in the EU, by a non-EU controller or processor, if the processing activities relate to: <ul style="list-style-type: none"> a) the offering of goods or services to a EU data subject; or b) the monitoring of a data subject's behaviour in the EU. 	<p>The APEC Framework defines personal information as any information about an identified or identifiable individual.</p> <p>The definition is intended to include information that would not meet the above criteria alone, but when put together with other information would identify an individual.</p> <p>The Framework is intended to apply to information about natural living persons, not legal persons.</p> <p>The ASEAN Framework does not have a definition.</p>	<p>Clear definition Personal data refers to any information, in electronic form or other form that is able to directly or in combination with other information identify an individual or reflects an identified individual's activities including but not limited to name, identification number, correspondence address, residential address, account information, financial information, and location data.</p>	<p>The PDP Bill defines "Personal Data" as "data of or about a natural person which makes her identifiable directly or indirectly (any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information, whether online or offline, and includes any inference drawn from such data for the purpose of profiling)."</p> <p>The Bill is applicable to (i) data used, shared, disclosed, collected or otherwise processed in India; (ii) data processed by an Indian citizen, company/ body established under Indian law, or the State; (iii) entities not based in India but which conduct activities like profiling, which could cause privacy harms to data principals in India, even if not based in India; (iv) entities not based in India but which carry on their business/ offers goods or services to data principals in India.</p> <p>Following an approach similar to the GDPR, the Bill shall be applicable to data fiduciaries not in India when, (i) personal data is processed in connection with business or service activities offered to data principals within the Indian territory, and (ii) activities involving profiling of data principals within the Indian territory. Companies incorporated in India would be subject to the Bill, regardless of where the actual processing/ storage etc. takes place.</p>	<p>The PDPO defines "Personal Data" as any data:</p> <p>(a) relating directly or indirectly to a living individual;</p> <p>(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and</p> <p>(c) in a form in which access to or processing of the data is practicable.</p> <p>The PDPO does not confer extra-territorial application and so the usual territorial principle should be applied in construing the provisions of the PDPO.</p>	<p>The PDPA defines "personal data" as data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which an organisation has or is likely to have access.</p> <p>The PDPA applies to all organisations which are not a public agency or acting on behalf of a public agency (no matter where incorporated) that collect, use or disclose personal data in Singapore.</p>	<p>The PDPA defines "Personal data" as, in the context of commercial activities, any information that relates directly or indirectly to an individual, where the individual is identified or able to be identified from that information, or from that information where combined with other information in the possession of a data user.</p> <p>The PDPA does not apply to the Federal and State Governments.</p> <p>The PDPA does not apply to personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia. In practice this intention can be construed as being at the point in time that the data is further processed in Malaysia where this cannot be clearly determined at the outset.</p>	<p>The PDPA defines "Personal Data" as information relating to a natural person which is directly or indirectly identifiable to such natural person, excluding information of a deceased person.</p>	<p>GR 71 defines Personal Data as every individual data which is identifiable and/or can be identifiable, alone or combined with other information, directly or indirectly, through an electronic system and/or non-electronic system.</p> <p>The EIT Law adopts the principle of extraterritoriality as it also applies (in theory) to any person who undertakes any relevant legal acts within or outside Indonesia, whether such person is based within or outside the territory of Indonesia and where such acts harm the "interest of Indonesia". The term "interest of Indonesia" is very broadly defined as Indonesian national economy interests, strategic data protection, the nation's dignity, state defense and security, sovereignty, citizen and legal entities, etc.</p> <p>The extraterritoriality principle as adopted by the EIT Law could be interpreted to mean that any implementing regulations under the EIT Law regime may also apply the extraterritoriality principle. The practice around this issue is yet to be confirmed.</p>	<p>The Data Privacy Act defines Personal Data as any information, whether recorded in a material form or not, from which the individual can be identified by the entity holding the information, or when put together with other information.</p> <p>Data Privacy act Section 6: "Extraterritorial Applications", states that the act applies to an act done or practice engaged in and outside of the Philippines by an entity if:</p> <p>(a) The act, practice or processing relates to personal information about a Philippine citizen or a resident;</p> <p>(b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following: (1) A contract is entered in the Philippines; (2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and (3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and</p> <p>(c) The entity has other links in the Philippines such as, but not limited to: (1) The entity carries on business in the Philippines; and (2) The personal information was collected or held by an entity in the Philippines.</p>	<p>Personal information is defined broadly by the Network Information Security (NIS) (86/2015/QH13) Law as information relating to the identity of a specific person. The personal information owner is the person identified by the personal information.</p> <p>This includes any information that relates to a data subject's:</p> <ul style="list-style-type: none"> Personal life, such as name, date of birth, address, telephone number, identification number, or email address. Personal or family secrets. Personal communications, including written correspondence and the content of telephone calls. 	<p>The Privacy Act defines "personal information" as information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion:</p> <ul style="list-style-type: none"> is true or not; and is recorded in a material form or not. 	<p>PDPA defines "personal data" refers to a natural person's name, date of birth, ID Card number, passport number, features, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, data concerning a person's sex life, records of physical examination, criminal records, contact information, financial conditions, data concerning a person's social activities and any other information that may be used to directly or indirectly identify a natural person;</p>	<p>Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances.</p> <p>For example, personal information may include:</p> <ul style="list-style-type: none"> an individual's name, signature, address, phone number or date of birth sensitive information credit information employee record information photographs internet protocol (IP) addresses voice print and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique) location information from a mobile device (because it can reveal user activity patterns and habits) <p>The Privacy Act 1988 doesn't cover the personal information of someone who has died.</p> <p>Ref: https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information/</p>	<p>Personal information includes any information about an identifiable individual, such as a name, date of birth, address, biometric information and/or gender etc. If there is a reasonable chance someone could be identified from the information, it is personal information. This also applies to individuals whose death is maintained pursuant to the Birth, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act.</p> <p>Application of principles to information held overseas</p> <p>(1) For the purposes of principle 5 (governs the way personal information is stored. It is designed to protect personal information from unauthorised use or disclosure.) and principles 8 to 11 (place restrictions on how people and organisations can use or disclose personal information. These include ensuring information is accurate and up-to-date, and that it isn't improperly disclosed.), information held by an agency includes information that is held outside New Zealand by that agency, where that information has been transferred out of New Zealand by that agency or any other agency.</p> <p>(2) For the purposes of principle 6 (gives individuals the right to access information about themselves.) and principle 7 (gives individuals the right to correct information about themselves.), information held by an agency includes information held outside New Zealand by that agency.</p> <p>(3) Nothing in this section shall apply to render an agency in breach of any of the information privacy principles in respect of any action that the agency is required to take by or under the law of any place outside New Zealand.</p>

	EU / UK	APEC Privacy Framework and the ASEAN Framework	China	India	Hong Kong	Singapore	Malaysia	Thailand	Indonesia	Philippines	Vietnam	Japan	Taiwan	Australia	New Zealand
6.	<p>Definition of 'Sensitive' personal data (or similar), and extraterritorial application/exclusions related to such definitions</p> <p>Article 9 of the GDPR defines "special category data" as personal data that:</p> <ul style="list-style-type: none"> • reveal racial/ethnic origin; • reveal political opinions; • reveal religious or philosophical beliefs; • reveal trade union membership; • genetic data; • biometric data for the purpose of identifying a person; • concerning health; • concerning a person's sex life; and • concerning a person's sexual orientation. <p>Criminal conviction data is also given additional protection under the GDPR, although it does not fall within the scope of special category data.</p> <p>Special category data under the GDPR does not include financial data or government issued ID documents and the list set out in Article 9 (as described above) is exhaustive.</p>	<p>N/A</p> <p>However, the APEC Framework provides that the credit card numbers, bank account information and sensitive personal information is referred to in discussion on obtaining data fairly and proportionally to what data will be used for.</p>	<p>No clear definition at law but there is a clear definition in the Personal Information National Standard and this is generally accepted.</p> <p>The Personal Information National Standard defines sensitive personal data as certain personal data that is highly critical and important to the data subject where any breach of such personal data, or unlawful collection or abuse of such personal data, will give rise to danger and impact to the data subject or his/her property, reputation, mental health, or will make the data subject to a victim of any discrimination. There is a non-exhaustive list of sensitive personal data under the Personal Information National Standard. Examples of sensitive personal data include identification card numbers, biometric data, bank account, communication records and details, property information, credit information, whereabouts, accommodation information, health and physiological information, transaction information and personal data of minors (below the age of fourteen).</p>	<p>The "PDP Bill" defines Sensitive Personal Data" as a sub-set of personal data that reveals, relates to or constitutes sensitive information such as financial information, health data, biometrics, official identifier, sex life, sexual orientation, transgender status, intersex status, genetic data, caste/ tribe, and religious/ political belief/ affiliation.</p> <p>The DPA is empowered to expand the scope of Sensitive Personal Data from time to time.</p> <p>Since the definition of financial information is broad and ambiguous, it could include credit card details, permanent account number details etc., which is routinely stored by financial institutions to facilitate know your customer checks and online transactions. This could pose challenges to businesses offering cross border payments to/from Indian entities.</p>	<p>Not applicable as 'sensitive personal data' is not defined in the PDPO.</p> <p>However additional guidance is issued for ID numbers and equivalent identifiers and consumer credit data.</p> <p>More specifically the Commissioner has clarified that biometric data should only be collected where it is necessary and with the consent of the data subject.</p> <p>There is no separate definition for sensitive personal information under the PDPO, and there are no categories of data set forth in the PDPO. For the definition of "personal data", please see row 5 above.</p> <p>To the extent that it would be practicable to ascertain a person directly or indirectly by virtue of such financial information then this would likely constitute personal data. Alternatively, if this was simply raw financial data alone and it is not possible to deduce who the person/customer is just by such financial information, then it would not constitute personal data under the PDPO.</p>	<p>Not applicable as "Sensitive" personal data is not defined under the PDPA.</p> <p>However, based on past decisions by the PDPC, certain types of personal data have been considered more sensitive than others and organisations that collect, use or disclose such personal data would generally be expected to provide more robust standards of protection. Such types of personal data include financial data, bankruptcy status and personal identifiers (eg, National Registration Identification Card and passport details).</p>	<p>The PDPA defines 'Sensitive personal data' as any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as may be determined by the Minister of Communications and Multimedia (nothing further actually issued).</p>	<p>Specific categories of personal data under Section 26 of the PDPA (which are subject to additional requirements in respect of collection and processing, even if not directly labelled "sensitive") include; personal data pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner, to be prescribed by the Committee (nothing further actually prescribed).</p>	<p>No definition of "sensitive" personal data (or similar terminology) is provided in the key regulations on data protection in Indonesia.</p> <p>The general data regulatory framework does not cover Gov ID info or financial info as such. Financial info is covered by financial services sectoral regulations outlined in response to no. 2 above.</p>	<p>Sensitive information, which is afforded additional protections, refers to personal information about an individual, such as race, ethnic origin, marital status, age, religion, philosophical or political affiliations, health, education, genetic or sexual life, legal proceeding, criminal history, social security number, health records, tax records, and classified information.</p> <p>Sensitive data may include data that harms the interests of the state/government of Vietnam or causes social instability. Personal data relating to religious or other beliefs or political opinions, for instance, may also be regarded as sensitive, the production, reproduction, access and dissemination of which is prohibited. The concept of "personal secrets" also exists under Vietnamese law and may refer to medical records, tax payment dossiers, social insurance card numbers, credit card numbers and others as defined by law. State agencies holding information classified as personal secrets may only supply or share such information with a competent third party in cases specified by law. If the sensitive data relates to state secrets, the information must be encrypted in network transmission and computer storage.</p>	<p>Sensitive information is recognized as a specific type of personal information, which includes information or an opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, health information and tax file number information.</p> <p>"Special care-required personal information" in this Act means personal information comprising a principal's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal</p> <p>According to "Guidelines for Personal Information Protection in the Financial Field" Article 6 Regarding Sensitive Information 1. An entity handling personal information in the financial field shall not acquire, use of provide to third party, information on political views, religion (meaning thoughts and creeds), participation in union activities, race, family origin and registered domicile, health care, sex life and past criminal records.</p>	<p>Data pertaining to a natural person's medical records, healthcare, genetics, sex life, physical examination and criminal records shall not be collected, processed or used unless on certain conditions are met.</p> <p>According to "Regulations Governing the Standards for Information System and Security Management of Electronic Payment Institutions" Article 10 "Sensitive data" include but are not limited to password, personal data, identity data, credit card number, credit card verification code, and personalized data.</p> <p>Ref: https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information/</p>	<p>Sensitive information is personal information that includes information or an opinion about an individual's:</p> <ul style="list-style-type: none"> • 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 • some aspects of biometric information <p>Generally, sensitive information has a higher level of privacy protection than other personal information.</p> <p>Health information is subject to specific protection through the Health Information Privacy Code (the "HIPC").</p>	<p>Not applicable as 'Sensitive' personal data (or similar) is not defined in the legislation. However, this is something that is assessed by the Privacy Commissioner on a case by case basis.</p> <p>The Privacy Act does not contain any concept or definition of sensitive personal data. However, the Privacy Act does require agencies collecting personal information to only do so for a "lawful purpose connected with a function or activity of the agency", and the collection must be "necessary" for that purpose (Privacy Principle 1). In addition, information may not be collected by unlawful, unfair or unreasonably intrusive means (Privacy Principle 4). In practice, this may constrain the collection of certain types of personal information where they cannot be reasonably connected to a lawful purpose of the agency.</p>	

	EU / UK	APEC Privacy Framework and the ASEAN Framework	China	India	Hong Kong	Singapore	Malaysia	Thailand	Indonesia	Philippines	Vietnam	Japan	Taiwan	Australia	New Zealand
7.	<p>Additional categories of data (e.g. 'critical' data or similar), and extraterritorial application/exclusions related to such data</p> <p><i>(Also states where critical data can overlap with personal or sensitive personal data)</i></p>	None – critical data is not a defined concept under the GDPR.	N/A	Unclear definition Important data is mentioned in the China Cyber Security Law but the definition of important data has not yet been finalized. Chinese regulators are still making rules on regulating the use and protection of important data.	Applicable but not clearly defined – “critical personal data” in Bill. The definition of “critical personal data” (which shall only be processed in India) will be notified in due course by the DPA. RBI sectoral rules define “Payment data” which must be localised.	None	None	None	<p>Yes, GR71 applies requirements to ‘strategic’ data.</p> <p>GR71 sets out that the Government will determine public institutions or institutions that own vital information infrastructure in certain sectors</p> <p>Sectors include:</p> <ol style="list-style-type: none"> 1. government administration 2. energy and mineral resources 3. transportation 4. financial 5. health 6. information and communication technology 7. food (resilience) 8. defence; and 9. other sectors that are specified by the President of Indonesia. 10. Regulatory guidance is needed on whether the definition of “institution” includes any ESO within the private scope. Further details are expected in an implementing regulation. 	<p>In DPA of the Philippines, the Privileged Information refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged information. (e.g. Attorney-Client Privilege, Certified Public Accountant Privilege)</p>	<p>The Vietnamese government labels information as state secrets when:</p> <ul style="list-style-type: none"> • The information relates to a case, a circumstance, a document, an object, a location, a time, or a speech that contains important content in the fields of: politics; national defense; national security; foreign affairs; economy; science; technology; or other subjects designated by the government. <p>The disclosure of the information may cause harm to the State of the Socialist Republic of Vietnam.</p>	None	None	None	None

<p>8. Grounds for collection and processing of personal data or transferring the same to third parties in the same jurisdiction</p> <p>(e.g. consent, legitimate business, compliance with applicable laws, outsourcing)</p>	<p>Article 6 sets out the six lawful basis of processing, being:</p> <ul style="list-style-type: none"> consent of data subject; necessary for the performance of a contract with the data subject or to take preparatory steps to such a contract; necessary for the compliance with a legal obligation; necessary to protect the vital interests of the data subject or another person; necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and necessary for the purposes of legitimate interests. 	<p>Lawful purpose and notice or consent where appropriate</p> <p>Under the APEC Framework, the collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.</p> <p>Data should be used for such notified purposes or other compatible or related purposes.</p> <p>Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.</p> <p>Under the ASEAN Framework an organisation should not collect, use or disclose personal data unless the individual is notified or given consent for such purpose or an available exemption applies.</p> <p>Collection, use or disclosure should only be for a purpose a reasonable person considers appropriate in the circumstances.</p>	<p>Under the China Cyber Security Law, consent is the legal basis.</p> <p>Compliance with laws and the performance of contract can also be legal basis which can be derived as a result of reconciliation of laws. There are other exemptions of consent requirements provided in the Personal Information National Standard but these are of no legal effect.</p>	<p>Consent</p> <p>Per the PDP bill, to process personal data, the data principal should have consented to such processing at the latest by the time the processing commences. There are no restrictions on intra-country transfer of personal data so long as consent has been obtained for such transfer from the Data Principal.</p> <p>The collection of personal data is permitted only to the extent necessary for the purposes of processing (e.g. necessary for the services to be provided). When a Data Fiduciary collects personal data, it is required to give clear and concise information about the collected data, purpose (of collection), nature and categories, details of data protection officer, process of consent withdrawal, consequences of non-provision of personal data, source, third party disclosure, cross-border transfer, period of retention, rights of data principals, grievance redressal process, right to complain to the DPA, and share any rating such as data trust score accorded to it, and any other information that the DPA prescribes.</p> <p>Exemptions</p> <p>For personal data, (but not sensitive personal data), where consent based processing would require efforts disproportionate to the sensitivity of such data or is necessary for recruitment, termination of recruitment, providing a service/ benefit to employees, attendance and assessing employee performance, the data fiduciary.</p> <p>Processing of personal data is also permissible if it is necessary for any legislative function (central or state), and State function authorised by law for (i) providing benefit/ service to the data principal, or (ii) issuing certification, license or permit to the data principal.</p> <p>[Please include exemptions such as those analogous to the Malaysia or EU columns if they are in the Bill].</p>	<p>Lawful purpose & notification</p> <p>For lawful purpose by lawful and fair means. Purpose of collection must be directly related to a function or activity of the data user (i.e. the person who controls the collection, holding, processing or use of personal data). The data collected should be necessary but not excessive in relation to that purpose.</p> <p>When personal data are collected from an individual, that person (the data subject) must be provided with the following information, which includes: (a) the purpose for which the data are to be used; (b) the classes of persons to whom the data may be transferred; (c) whether it is obligatory or voluntary for the data subject to supply the data; (d) the consequences arising if the data subject fails to supply the data; and (e) the data subject has the right to request access to and correction of the data.</p> <p>Consent for direct marketing</p> <p>Separately, the PDPO has strict requirements relating to direct marketing. A data user must obtain consent of the data subject to the proposed direct marketing activities.</p> <p>Exemptions</p> <p>Exemptions for complying with certain data protection principles in the PDPO include:</p> <p><i>Purpose of prevention or detection of crime, prevention or remedy of unlawful conduct.</i></p> <p><i>Purpose of assessment or collection of tax.</i></p> <p><i>Required in connection with legal proceedings in Hong Kong or exercising or defending legal rights in Hong Kong.</i></p> <p><i>Due diligence for proposed M&A.</i></p> <p><i>Certain employment situations such as staff planning</i></p>	<p>Consent</p> <p>Generally, an organisation would need to obtain an individual's consent for the collection, use or disclosure of his personal data for a specified purpose unless it is required under any law, or an exception under the PDPA applies.</p> <p>Exemptions under the PDPA</p> <p>Exemptions include:</p> <p><i>Disclosures relating to an investigation or proceeding or provision of legal service</i></p> <p><i>Managing employee relationships</i></p> <p><i>Relating to M&A ("business asset transactions")</i></p> <p><i>Carrying out research, journalistic, literary or artistic purposes.</i></p> <p>Reasonableness (even with consent)</p> <p>Organisations should not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal data beyond what is reasonable to provide such product or service.</p>	<p>Consent</p> <p>Consent of data subject usually required subject to limited exemptions.</p> <p>Exemptions</p> <p>Exemptions include where processing is necessary:</p> <p>(a) for the performance of a contract to which the data subject is a party;</p> <p>(b) for the taking of steps at the request of the data subject with a view to entering into a contract;</p> <p>(c) for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract;</p> <p>(d) in order to protect the vital interests of the data subject;</p> <p>(e) for the administration of justice; or</p> <p>(f) for the exercise of any functions conferred on any person by or under any law.</p> <p>Section 45 of the PDPA provides further partial exemptions from certain data protection principles in relation to the processing of personal data, e.g. in respect of the prevention or detection of crime, assessment or collection of any tax or duty, preparing statistics or carrying out research, discharging regulatory functions, journalistic, literary or artistic purposes.</p>	<p>Consent</p> <p>Data controller must obtain an individual's consent except where relevant exemptions apply. Data controller must inform the data subject: (i) the purposes of collection; (ii) the data to be collected; (iii) the rights of the data subject; and so forth.</p> <p>Legitimate interests of data controller</p> <p>Consent is not needed where the relevant activity is necessary for the legitimate interest of the data controller or any other persons other than the data subject, except where such interests are overridden by the fundamental rights of the data subject of his or her personal data.</p> <p>Exemptions</p> <p>Exemptions include where processing is necessary:</p> <p>(a) for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;</p> <p>(b) it is necessary for compliance with a law to which the data controller is subjected.</p>	<p>Consent and / or specific purpose</p> <p>Under GR 71 and Regulation 20, consent must be conveyed explicitly, clearly and must not be based on fault, negligence, or coercion. Consent may not be implicit or "passive" (e.g. the privacy policy shall apply whenever a user utilises the services provided by the relevant ESO). The consent will need to be given in writing (electronically or manually) and in Bahasa Indonesia form (or bilingual version.)</p> <p>The exemptions available are very limited and narrow. Exemptions to providing consent apply in law enforcement type scenarios. For example, if required by Indonesian court or authorities, if requested by law enforcement officers in relation to criminal allegations, or if otherwise required under Indonesian laws.</p> <p>Additional Requirements</p> <p>In addition to obtaining consent from personal data owners, GR 71 requires ESOs must process personal data for one of the following specific purposes:</p> <ol style="list-style-type: none"> to satisfy contractual obligations under an agreement entered into by the personal Data Owner, or to fulfil a request from the personal Data Owner at the time the parties enter into the agreement; to satisfy any legal obligations of the data controller contained in any applicable regulations; to implement the authority of the data controller under applicable regulations; to satisfy the obligations of the data controller in the context of public service for the interest of the public; and/or to satisfy any other lawful interest of the personal data controller or owner. <p>Based on the strict wording of GR 71, it appears that the above are additional to the consent requirement, rather than additional exemptions from obtaining written consent as such. However, based on verbal discussions with MOCI officials, we understand that these should be interpreted as exemptions from the consent requirement. This may be clarified in the next draft of the bill.</p>	<p>Collection and Notice</p> <p>When collecting personal information, data must be:</p> <ul style="list-style-type: none"> Collected only for a specific and legitimate purpose determined and declared. Accurate, relevant and kept up to date where necessary for the declared purpose. Adequate and not excessive in relation to the declared purpose. De-identified when no longer necessary for the declared purpose. <p>The data subject is entitled to be informed of:</p> <ul style="list-style-type: none"> The purpose for which the personal information is being collected. The scope and method of processing. The recipients or classes of recipients to whom personal data will be disclosed. Methods to access data. The identity and contact details of the data controller. The period for which the data will be stored. Any rights the data subject may have. <p>Data subjects shall be notified and given an opportunity to withhold consent in case of any changes to the information declared to the data subject since consent was sought.</p> <p>Use and Disclosure</p> <p>Personal information must be accurate and relevant. It must only be processed fairly, lawfully, in a way compatible with the declared purpose and in a manner that ensures appropriate privacy and security safeguards. Processing of personal data shall adhere to the principles of transparency, proportionality. Processing personal information is only lawful and permitted where the data subject has consented, or it is necessary:</p> <ul style="list-style-type: none"> For the processor to fulfil a contract with the data subject. For the controller to comply with legal obligations. To protect the data subject's life and health. To respond to a national emergency, uphold public order and safety, or fulfil functions of a public authority. As the legitimate interests of the controller or third parties override the data subject's rights. <p>Sensitive information must not be processed unless the data subject has consented, or it is necessary:</p> <ul style="list-style-type: none"> To fulfil rights or obligations under existing laws and regulations. To protect the life and health of the data subject or another person. To achieve the lawful and non-commercial objectives of public organisations. For purposes of medical treatment, and adequate level of protection is ensured. 	<p>Collection and Notice</p> <p>The NIS Law requires that when collecting personal information, organisations and individuals must collect personal information only after obtaining the consent of the information owner on the scope and purpose of the information collection and use</p> <p>Use and Disclosure</p> <p>The NIS Law requires that when collecting or using personal information, organisations and individuals must only use collected personal information for any purpose different from the initial one only after obtaining the personal information owner's consent. They must not share or disclose personal information to any third party, unless it is agreed by the personal information owner or requested by competent state bodies.</p> <p>Vietnamese law defines persons 16 years old or younger to be minors. To process the personal data of a minor, an organization must obtain the consent of the minor's parent or guardian.</p> <p>The law defines processing personal data as engaging in one or more of the following activities with personal data:</p> <ul style="list-style-type: none"> Collecting. Editing. Using. Storing. Providing to any third party. Transferring. Sharing. Publishing. 	<p>The APPI refers to the collection of personal information as proper acquisition. PIHBOs must not obtain personal information by deceit or improper means. PIHBOs must promptly and explicitly inform the principal whose personal information was acquired of the utilisation purpose, including where the purpose has changed. However, this notice requirement does not apply in cases where there exists an urgent need to protect human life, body or fortune, or where the utilisation purpose was previously disclosed to the public. PIHBOs must obtain the principal's consent before collecting sensitive information.</p> <p>(Also see #9 below – further about transferring personal data to third party)</p>	<p>Collection and notice</p> <p>Collection of data is defined as 'to collect personal information in any form and way'. The collecting of data should be:</p> <ul style="list-style-type: none"> Respectful of the rights and interests of the data subject, Following 'bona fide', Reasonable and fair, and Limited to the purpose of collection. <p>On collecting data, the organisation is required to inform data subjects of the:</p> <ul style="list-style-type: none"> Organisation name, Purpose of data collection, Classification, Time, location, receiver and uses of data, Data subject's rights, and Consequences if they choose not to provide the personal information. <p>Use and disclosure</p> <p>Lawful use of data differs between government and non-government agencies. In Taiwan, data processing is defined as actions to record, input, store, compile, correct, duplicate, retrieve, delete, output, connect or internally transmit information to establish or use a personal information file. Data use is defined as all personal information use that is not covered under processing (as above). Government or Non-government agencies must comply with at least one of the following clauses before processing information:</p> <ul style="list-style-type: none"> when in accordance with law; when the collection of personal information is necessary for the government agency to perform its official duties or the non government agency to fulfill the legal obligation; when the notice will impair the government agency in performing its official duties; when the notice will impair public interests. when the Party should have known the content of the notification already; when the collection of personal information is for non-profit purposes and clearly does not cause any detriment to the Party. <p>Personal data may only be used for the purpose of collection, unless accepted by the PDPA.</p> <p>(Also see #9 below – further about transferring personal data to third party)</p>	<p>An organisation or agency must only collect personal information in a lawful and fair way. If practical, they must collect the information from you personally and not from third parties. But there are situations where organisations and agencies are allowed to collect information about you from third parties. For example:</p> <ul style="list-style-type: none"> where you would reasonably expect it or where you've consented to your personal information being shared a law enforcement agency may collect personal information about an individual who is under investigation without asking the individual directly because to do so may jeopardise the investigation if a legal or official document mailed to an individual is returned to the sender, then the sender may need to get the individual's current contact details from another source <p>An entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. The exceptions include where:</p> <ul style="list-style-type: none"> the individual has consented to a secondary use or disclosure the individual would reasonably expect the entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order a permitted general situation exists in relation to the secondary use or disclosure the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure the entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted 	<p>Collection of data according to the New Zealand Privacy Act:</p> <p>Personal information shall not be collected by any agency unless—</p> <p>(a) The information is collected for a lawful purpose connected with a function or activity of the agency; and</p> <p>(b) The collection of the information is necessary for that purpose.</p> <p>Furthermore, the agency collecting data from an individual will inform the data subject of the fact of collection, the intended use of the information and the recipients of the information. The agency will also inform the data subject of their rights of access and correction. Agencies will not obtain information by illegal means or to an unreasonably intrusive extent.</p> <p>An approved information sharing agreement may authorise an agency to share any personal information with 1 or more other domestic agencies in accordance with the terms of the agreement.</p>
--	---	---	--	---	---	---	--	---	---	---	--	---	---	--	---

EU / UK	APEC Privacy Framework and the ASEAN Framework	China	India	Hong Kong	Singapore	Malaysia	Thailand	Indonesia	Philippines	Vietnam	Japan	Taiwan	Australia	New Zealand
									<ul style="list-style-type: none"> For the protection of lawful rights and interests of individuals. <p>Consent to the processing of personal and sensitive information must be freely given, specific, informed, and evidenced by written, electronic or recorded means.</p>				<ul style="list-style-type: none"> by, or on behalf of, an enforcement body, or the entity is an agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner. <p>Ref: https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/collection-of-personal-information/</p>	

<p>9.</p>	<p>Grounds for cross-border transfer of personal data</p> <p>(e.g. consent, legitimate business, compliance with applicable laws, outsourcing)</p>	<p>Under GDPR, transfer is permitted if:</p> <ul style="list-style-type: none"> the country, territory or international organisation receiving the personal data is covered by an EU Commission's "adequacy decision"; the transfer is subject to one of the below "appropriate safeguards" identified by the GDPR: <ul style="list-style-type: none"> a) a legally binding & enforceable instrument between public authorities/bodies; b) Binding corporate rules (for intra-group transfers); c) Standard Contractual Clauses (approved by the EU Commission); d) Standard data protection clauses adopted by a supervisory authority and approved by the Commission (no supervisory body has yet adopted such clauses); e) an approved code of conduct; f) an approved certification mechanism; or g) one of the 'derogations' listed in Article 49 applies. 	<p>APEC jurisdictions should endeavour to ensure that cross-border privacy rules and recognition or acceptance mechanisms facilitate responsible and accountable cross-border data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessary administrative and bureaucratic burdens for businesses and consumers.</p> <p>No restriction on cross border data transfers but entities must recognise the interests of individuals to legitimate expectations of privacy under a principle of preventing harm. This is in addition to the lawful and fair requirements (and notice and consent where appropriate). Notice should include the identity and location of personal information controllers.</p> <p>Under the ASEAN Framework, before transferring personal data to another country or territory, the organisation should either obtain the consent of the individual for the overseas transfer or take reasonable steps to ensure that the receiving organisation will protect the personal data consistently with the framework. ASEAN has proposed a draft cross border mechanism based on certification and contractual clauses. The expectation is that the details of this mechanism will be worked out during 2020.</p> <p>An ASEAN Data Management Framework (DMF) has also been proposed which will set guidelines for how companies handle the data they hold. Adhering to these standards may be a precondition for data flowing across borders.</p>	<p>Pre-approval on a per-transferee basis</p> <p>Under the China Cyber Security Law, the rules on cross-border data transfer have not yet been finalized for network operators in general (excluding critical information infrastructure operators).</p> <p>Please note that the draft Measures for Security Assessment for Cross-border Transfer of Personal Data provide relevant obligations on the network operator to submit the proposed cross-border transfer of personal data to CAC for security assessment. It is likely that in near future the cross-border transfer of personal data by network operators would also need to pass the security assessment. Please note that the new draft measures seem to favor the approach of having a contractual arrangement to ensure the overseas data receiver must protect the personal data and facilitate the exercise of data subject rights. Some mandatory clauses have been proposed for such cross-border data transfer agreements, such as that the network operator in China shall first compensate the data subject in the event of infringement of the right to data protection by the overseas data receiver, unless the network operator can prove that it is not at fault.</p> <p>While the new draft measures have not been finalized, the network operators in China may conduct the cross-border transfer of personal data provided that self-assessment is completed and consent of data subjects concerned is obtained.</p> <p>Sectoral rules in the financial services industry provide a general data localization requirement on personal financial data. Personal financial data that is collected in China shall be stored, processed and analysed in China. The Banking financial institutions are prohibited from transferring personal financial data outside China unless relevant conditions are met, i.e. (i) this cross-border data transfer is necessary for the domestic financial institutions to provide relevant cross-border business to the financial customers and the authorization of the financial customers is obtained; (ii) the offshore data receivers are limited to certain types of affiliated entities of the domestic financial institutions (i.e. it's headquarter, parent company, branch company, subsidiary or other affiliated entities that are necessarily needed for the completion of the cross-border business concerned); and (iii) the domestic financial institutions shall request the offshore data receivers to protect the transmitted personal financial data by means of concluding contract, conducting onsite inspection and other sufficient measures.</p> <p>Sectoral rules in the financial services industry prohibit the banking financial institutions from transferring client identification materials and transaction information that are collected by the banking financial institutions during the process of anti-money Laundering and counter-terrorist financing to a place outside China unless permitted by laws and administrative regulations.</p>	<p>The PDP Bill permits the cross-border transfer of personal data in furtherance of the purpose for which it was collected, assuming that consent was validly obtained from the Data Principal.</p>	<p>Consent and ensuring equivalent protection in third country</p> <p>Section 33 of the PDPO sets out restrictions on cross-border transfers of personal data but it is not yet in force.</p> <p>Section 33 covers transfers from Hong Kong to a place outside Hong Kong and transfers between two other jurisdictions where the transfer is controlled by a Hong Kong data user.</p> <p>If and when section 33 comes into effect, the transfer of personal data to places outside Hong Kong is prohibited unless at least one of the following conditions are met. The conditions are that:</p> <ul style="list-style-type: none"> the destination has been approved by the Privacy Commissioner in writing; the data user has reasonable grounds for believing that the place has privacy laws which are substantially similar to, or serve the same purpose as, the PDPO; the individual has consented in writing to the transfer; the data user has reasonable grounds for believing that the transfer is for the avoidance or mitigation of adverse action against the data subject; it is not practicable to obtain the data subject's consent but, if practicable, such consent would be given; the data are exempt from Data Protection Principle 3 by virtue of Part VIII of the PDPO which exempts personal data held for certain purposes such as domestic purposes, employment or staff planning, the prevention or detection of crime, the security or defence of Hong Kong, legal professional privilege, news activities etc; the data user has taken "all reasonable precautions and exercised all due diligence to ensure" that the data will not be collected, held, processed or used in any manner that would constitute a contravention of the PDPO if it occurred in Hong Kong. <p>While section 33 has not come into force, the PDPC has mentioned that data users should comply with the good practice recommendations stated in its guidance on cross border transfer, being:</p> <ul style="list-style-type: none"> Reviewing any data transfer arrangements 	<p>Same as domestic transfers, plus ensuring equivalent protection in third country.</p> <p>Obtain individual's consent for the disclosure of his personal data for a specified purpose to an overseas recipient unless it is required under any law or an exception under the Fourth Schedule of the PDPA applies.</p> <p>Pursuant to a "transfer limitation obligation" under the PDPA, organisations transferring personal data abroad must do so in accordance with the requirements prescribed under the PDPA to ensure that the recipient provides a standard of protection to personal data so transferred that is comparable to the protection under the PDPA.</p> <p>One way to achieve this is as follows:</p> <ul style="list-style-type: none"> For inter-corporate transfers: data transfer agreement For intra-corporate transfers: binding corporate rules 	<p>Generally same as domestic transfers, or ensuring equivalent protection in third country.</p> <p>PDPA requires that transfers of personal data overseas be conducted only with the consent of the data subjects or where such other exceptions apply (e.g. where the transfer is necessary for the performance of contract, or where reasonable precautions or due diligence have been exercised to ensure that personal data will not be processed in the recipient jurisdiction in such manner which contravenes the PDPA, etc.).</p>	<p>Generally same as domestic transfers. Alternative methods not yet finalized.</p> <p>An additional ground that can be relied upon is where the destination country or international organization that receives such Personal Data has adequate data protection standards, and the transfer complies with additional rules for the protection of Personal Data to be prescribed by the PDPC. However the PDPC has not yet prescribed any such rules.</p> <p>Another ground for cross border transfers is an intragroup transfer where 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 Committee have been provided by the Data Controller or the Data Processor. However the PDPC has not yet prescribed any rules.</p>	<p>Notification and Reporting</p> <p>In addition to requirements applicable to domestic transfers, Regulation 20 provides that cross border transfer of personal data must be notified to the MOCI. Such notification should contain the following the minimum information:</p> <ol style="list-style-type: none"> name of the country of destination; name of the recipient; date of transfer; and reason(s) or purpose(s) for such transfer of Personal Data. <p>Such notification should be notified to MOCI prior to the transfer of such data, and ESOs are to provide a report on the result of such overseas transfer activity.</p> <p>Based on a no-name basis informal consultation with officials at MOCI, such notification may be provided once (i.e. at the beginning) in the event that the transfer of Personal Data is to be conducted on a routine basis (e.g., multiple transfers hourly, daily, weekly etc.), assuming that the notification indicates that the transfer shall be conducted on a routine basis. Officials at MOCI have verbally confirmed on an informal basis that a report recording all such overseas data transfers should be provided to MOCI thereafter on an annual basis for the preceding 12 month period along with a plan for the next 12 month period.</p>	<p>Cross-border Data Transfer</p> <p><i>Private Sector</i></p> <p>Before sharing data, controllers must obtain consent from the data subject and provide details of the transfer including relevant data, recipients and the data subject's rights. Consent is required even when the data is to be shared with an affiliate or parent company, or similar relationships. Data-sharing for commercial purposes, including direct marketing, is to be covered by a data-sharing agreement, which establishes adequate safeguards for data privacy and security. The data-sharing agreement shall be subject to review by the Commission, on its own initiative or upon complaint of data subject.</p> <p><i>Public sector</i></p> <p>Data-sharing between government agencies pursuant to a public function or service shall be covered by a data-sharing agreement guaranteeing compliance with the Act, including safeguards for data privacy and security. The data-sharing agreement shall be subject to review by the Commission, on its own initiative or upon complaint of data subject.</p>	<p>There are no specific restrictions on the cross-border transfer of personal information in Vietnam. However, the Law on Cybersecurity requires that organizations must not share personal information to any third party, unless it is agreed by the individual or requested by competent state bodies. There are no specific restrictions or requirements in Vietnam which apply to cross-border transfers of personal information.</p>	<p>Personal information must not be transferred to a third party unless consent has been obtained from the principal or any one of the above exceptions apply, as provided within 'Collection and notice'. Personal information may be transferred outside of Japan where:</p> <ul style="list-style-type: none"> Consent is obtained from the principal. The foreign state has privacy laws which are considered equivalent to Japan. The foreign party maintains an internal personal information protection system consistent with standards set by the PPC. <p>If one of the followings has occurred when the non-government agency transmits personal information internationally, the government authority in charge of subject industry may limit its action:</p> <ol style="list-style-type: none"> Where it involves major national interests; Where national treaty or agreement specifies otherwise; Where the country receiving personal information lacks of proper regulations towards the protection of personal information and it might harm the rights and interests of the Party; Where international transmission of personal information is made through an indirect method in which the provisions of this Law may not be applicable. <p>Cross border transfer in Taiwan is generally permitted. There are no data transfer agreements. Exceptions to this are</p> <ul style="list-style-type: none"> Biological specimens in a biobank International transmission of biobank data must be approved by the Ministry of Health and Welfare Financial Supervisory Commission approval is required to outsource retail operations Telecommunications providers cannot transfer data to China 	<p>Data transfer</p> <p>When disclosing to third parties, organisations are required to ensure the protection of personal information. If information is shared to third parties, the organisation and third party are both liable for data breaches by the third party.</p> <p>Before an entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to the information.</p> <p>An entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the Principles.</p> <p>There are some exceptions to these requirements in the Australian Privacy Act 1988.</p> <p>Ref: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information/</p>	<p>The Privacy (Cross-Border Information Amendment) Act 2010 states that the Privacy Commissioner may prohibit cross-border transfer of personal information if:</p> <ol style="list-style-type: none"> The Commissioner suspects with reasonable grounds that the information may be being 'routed' through New Zealand into a state where it will not be protected by substantial privacy legislation; The transfer would contravene the principles of the Organisation for Economic Co-operation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. <p>Proposal in the Privacy Bill 2020 - Disclosing information to an agency overseas</p> <p>The proposed IPP 12 (which is based on IPP 11(3) to (6) in the bill as introduced) sets out the principles for disclosure of personal information outside New Zealand. In most cases, an agency that wants to disclose personal information to a foreign person or entity would need to satisfy at least one of the criteria set out in our proposed IPP 12(1):</p> <ul style="list-style-type: none"> the individual concerned authorises the disclosure, after being expressly informed by the agency that the foreign person or entity may not be required to protect the information in a way that, overall, provides comparable safeguards to those in the bill the foreign person or entity is carrying on business in New Zealand, and the agency believes, on reasonable grounds, that the foreign person or entity is subject to the bill the agency believes on reasonable grounds that the foreign person or entity is a participant in a prescribed binding scheme the agency believes on reasonable grounds that the foreign person or entity is subject to privacy laws of a prescribed country the agency otherwise believes on reasonable grounds that the foreign person or entity must protect the information in a way that, overall, provides comparable safeguards to those in the bill. <p>It is recommended to include the fourth criterion as it is believed that the new IPP 12 should also allow for possible future participation by New Zealand in binding cross-border privacy</p>
-----------	---	---	---	--	--	--	--	---	---	--	---	---	--	---	--

	EU / UK	APEC Privacy Framework and the ASEAN Framework	China	India	Hong Kong	Singapore	Malaysia	Thailand	Indonesia	Philippines	Vietnam	Japan	Taiwan	Australia	New Zealand	
					<ul style="list-style-type: none"> Control of cross-border data flow activities Consider if any exceptions to section 33 applies including checking the White List published by the PDPC Keep an inventory of personal data being transferred outside of Hong Kong Conduct regular audits and inspections on transferees' operations to ascertain their compliance with their obligations under the data transfer agreement 											<p>schemes. An example of such a binding scheme is the Asia Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system. Six out of the 21 APEC economies participate in the system. We recommend inserting a definition of "country" into clause 6 which includes a state, territory, province, or any other part of a country.</p> <p>Criteria for prescribing binding schemes and countries</p> <p>It is recommended inserting new clauses 212A and 212B to provide for the making of regulations prescribing countries and binding schemes for the purposes of IPP 12, and to set out the criteria that the Minister must consider before recommending that such 6 Privacy Bill Commentary regulations be made. The Minister would be able to recommend that countries or binding schemes be prescribed if satisfied that personal information would be subject to privacy safeguards that are, overall, comparable to those in the bill.</p>

	EU / UK	APEC Privacy Framework and the ASEAN Framework	China	India	Hong Kong	Singapore	Malaysia	Thailand	Indonesia	Philippines	Vietnam	Japan	Taiwan	Australia	New Zealand	
10.	<p>Additional grounds for collection, processing, or transfer of sensitive or critical data (either in the same jurisdiction or on a cross-border basis)</p>	<p>Under Article 9, special category data can only be processed if one the below conditions are satisfied:</p> <ul style="list-style-type: none"> explicit consent has been given by the data subject; processing is necessary: <ul style="list-style-type: none"> a) for employment, social security and social protection (if authorised by law); b) to protect the vital interests of the data subject or another person; c) for establishment, exercise or defence of legal claims or judicial acts; d) for reasons of substantial public interest (with a basis in law); e) for the purposes of health or social care (with a basis in law); f) for reasons of public health (with a basis in law); or g) for archiving, research and statistics purposes (with a basis in law); not-for-profit bodies; and personal data made public by the data subject. <p>Member States are also able to set additional grounds for processing special category in national legislation.</p>	<p>N/A although note that given the general principles relating to proportionality, businesses should take into account that more sensitive data needs more proportionate protection in terms of lawful and fair use, notice and protection of legitimate expectation of privacy.</p>	<p>There have been a draft of measures released by Cyberspace Administration of China that proposed filing requirement for the collection of important data and sensitive personal data for business purpose.</p> <p>These draft measures also required the publication, share, trade, or cross-border transfer of important data to be subject to relevant security assessment and approval of supervisory authorities.</p>	<p>Sensitive Personal Data may be transferred outside India with explicit consent and (i) approved intra-group schemes, (ii) permitted countries/organisations, (iii) specific transfer(s) based on necessity approved by the DPA.</p> <p>As the definition of Sensitive Personal Data includes financial data, a much broader subset of data for financial institutions will be subject to explicit consent for cross border transfers. Currently, under the SPDI Rules, the transfer of 'sensitive personal data or information' by a body corporate is permissible if it is necessary for the performance of a lawful contract or is affected pursuant to the consent of the provider of information.</p> <p>A copy of such Sensitive Personal Data is required to be stored in India.</p> <p>Critical Personal Data (the definition of which the DPA may notify) shall only be processed and stored within India.</p>	N/A	N/A	N/A	<p>Explicit consent is generally needed for sensitive personal data.</p> <p>Any collection / transfer of 'sensitive' personal data can be done without the explicit consent from the data subject in certain cases, including where:</p> <p>(a) it is necessary for the establishment, compliance, exercise or defense of legal claims;</p> <p>(b) it is necessary for compliance with certain laws on health, employment and other matters as set out in section 26 of the PDPA.</p>	<p>Nothing additional to the above.</p>	<p>In the Implementing Rules and Regulation of the DPA, on Section 13: <i>Sensitive Personal Information and Privileged Information</i>, it states that The processing of sensitive personal and privileged information is prohibited, except in any of the following cases:</p> <p>a. Consent is given by data subject, or by the parties to the exchange of privileged information, prior to the processing of the sensitive personal information or privileged information, which shall be undertaken pursuant to a declared, specified, and legitimate purpose;</p> <p>b. The processing of the sensitive personal information or privileged information is provided for by existing laws and regulations: Provided, that said laws and regulations do not require the consent of the data subject for the processing, and guarantee the protection of personal data;</p> <p>c. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;</p> <p>d. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations provided that:</p> <ol style="list-style-type: none"> Processing is confined and related to the bona fide members of these organizations or their associations; The sensitive personal information are not transferred to third parties; and Consent of the data subject was obtained prior to processing; <p>e. The processing is necessary for the purpose of medical treatment: <i>Provided</i>, that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured; or</p> <p>f. The processing concerns sensitive personal information or privileged information necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.</p>	None	N/A	N/A	N/A	<p>No Definition</p> <p>None - 'sensitive or 'critical' data is not a defined concept under the NZ Privacy Act.</p> <p>The Privacy Commissioner may authorise the collection, processing or transfer of personal information in breach of the normal Privacy Act principles if:</p> <p>(a) The public interest in that collection or, as the case requires, that use or that disclosure outweighs, to a substantial degree, any interference with the privacy of the individual that could result from that collection or, as the case requires, that use or that disclosure; or</p> <p>(b) That collection or, as the case requires, that use or that disclosure involves a clear benefit to the individual concerned that outweighs any interference with the privacy of the individual that could result from that collection or, as the case requires, that use or that disclosure.</p>

	EU / UK	APEC Privacy Framework and the ASEAN Framework	China	India	Hong Kong	Singapore	Malaysia	Thailand	Indonesia	Philippines	Vietnam	Japan	Taiwan	Australia	New Zealand		
11. Other	Duplicative, inconsistent or supplementary rules relating to collection, processing or cross-border transfer of data and/or other complexities	None	N/A	Complexity across various laws and regulations; overlapping regulators There is some duplication of rule-making by various ministries. In general, the data protection rules making is co-ordinated by Cyberspace Administration of China and sectoral regulators are also making rules in light of these general principles as consensus.	Not clear how rules relating to "critical" "payment" or "sensitive" data relating to financial services will interact. RBI had released a notification on 6 April 2018, requiring that all data relating to payment systems in India be located solely in India . The rationale which the notification outlined was "monitoring" and "unfettered supervisory access". The notification was succeeded by stakeholders voicing concerns over compliance and technical challenges, all of which required additional clarity from the RBI. To this end, the RBI published a set of FAQs on 26 June 2019. The FAQs permit processing of financial data outside India, provided (1) post processing, the data is stored only in India (including end to end transaction details), (2) the data is moved to India and deleted from any foreign systems within 24 hours of payment processing, (3) for related processing activities (such as chargebacks), remote access to data located in India is permitted. Given that there is likely to be an overlap between payment data which the RBI seeks to localise, and Sensitive Personal Data as defined in the PDP Bill, there is likely to be a conflict between the localisation mandated by the RBI and the transfers permitted by the PDP Bill insofar as such 'payment data' relates to natural persons.	The SFC issued a circular on 31 October 2019 ("Circular") setting out the regulatory requirements for licensed corporations ("LCs") when using electronic data storage providers ("EDSPs"). EDSPs include public and private cloud services providers, as well as external providers of data storage at conventional data centres or other forms of virtual storage. The Circular reminds LCs of their obligation to ensure the preservation and integrity of those records or documents they are required to keep under the Securities and Futures Ordinance ("SFO") and the Anti-Money Laundering and Counter-Terrorist Financing Ordinance ("Regulatory Records"). The Circular applies to LCs who rely on EDSPs either exclusively or in conjunction with on-site data hosting. Unless the LC keeps its Regulatory Records simultaneously at its approved premises in Hong Kong, the LC needs to comply with Sections C, D and E of the Circular. All LCs that use EDSPs, regardless of whether Regulatory Records are kept exclusively with an EDSP, must comply with Section E of the Circular (General obligations of LCs using external data storage or processing services). If the EDSP is a Hong Kong EDSP, the LC is required to issue a notice ("Notice") to the EDSP authorising the EDSP to provide the Regulatory Records of the LC to the SFC. If the EDSP is a non-Hong Kong based entity, it must provide an undertaking ("Undertaking") to provide Regulatory Records and assistance as may be required by the SFC. The EDSP would be consenting to assisting the SFC in exercising its statutory powers despite the fact that the EDSP is an offshore entity. The LC is also required to issue the Notice to the EDSP. The rationale behind the Undertaking and Notice is to empower the SFC to be able to promptly access the LC's Regulatory Records without undue delay, and to be sure of the authenticity, integrity and reliability of the Regulatory Records. The SFC also indicated in its Circular that the production of these records may be required to be produced in legal proceedings initiated by the SFC or the Department of Justice in Hong Kong. There are also requirements on LCs to ensure that a proper audit trail exists regarding any access to the Regulatory Records when stored with their EDSP. LCs also need to designate two managers-in-charge that would be based in Hong Kong (who would be the responsible point of contact for the SFC).	The PDPA provides that the provisions of other written law prevail over portions of the PDPA to the extent of any inconsistency. E.g., MAS Notice to Banks on Prevention of Money Laundering and Countering the Financing of Terrorism ("MAS 626") states that in the course of performing customer due diligence in compliance with MAS 626, banks may be required to collect, use and disclose personal data of individuals without first obtaining consent. In this case, MAS 626 will prevail over the requirement to obtain an individual's consent for the collection, use or disclosure of his personal data for a specified purpose under the PDPA. The supplementary regulations issued under the PDPA are: • Personal Data Protection (Composition of Offences) Regulations 2013 • Personal Data Protection (Do Not Call Registry) Regulations 2013 • Personal Data Protection (Enforcement) Regulations 2014 • Personal Data Protection Regulations 2014 • Personal Data Protection (Appeal) Regulations 2015	The Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 ("AMLAATFA") stipulates that any secrecy obligations imposed by any written law are overridden by the reporting obligations under the AMLAATFA on reporting institutions such as licensed banks. The subsidiary legislation to the PDPA are the Personal Data Protection Regulations 2013, Personal Data Protection (Registration of Data User) Regulations 2013, Personal Data Protection (Class of Data Users) Order 2013, Personal Data Protection (Fees) Regulations 2013, Personal Data Protection (Compounding of Offences) Regulations 2016 and Personal Data Protection Standard 2015.	In the event that there is any sector-specific law governing the protection of Personal Data in any manner, any business or any entity, the provisions of such law should prevail, except for: 1. in relation to collection, use, or disclosure of Personal Data, 2. the provisions with respect to the rights of data subjects including relevant penalties, 3. where the PDPA's expert committee has powers to protect data subjects which are greater than analogous powers provided to authorities in other legislation, In which case the PDPA can supersede the other sector-specific law.	1. The implementation and enforcement of the extraterritorial principle is difficult in practice. We have not seen any real-world examples to date. 2. GR 71 is recently issued and as such the implementing regulations of the GR 71 will be issued to provide more detail on how to implement the obligations set out under GR 71 3. Please see possible different implementation of GR 71 in practice in relation to the ability to process personal data based on other reasons as set out in item 1 to 6 in the response of item 8 without consent.	The supplementary regulations issued under the Philippines DPA are: • NPC Circular 16-01 – Security of Personal Data in Government Agencies • NPC Circular 16-02 – Data Sharing Agreements Involving Government Agencies • NPC Circular 16-03 – Personal Data Breach Management • NPC Circular 16-04 – Rules of Procedure • NPC Circular 17-01 – Registration of Data Processing Systems • NPC Circular 17-01 Appendix 1 – Registration of Data Processing Systems Appendix 1 • NPC Circular 18-01 – Rules of procedure on requests for Advisory Opinions • NPC Circular 18-02 – Guidelines on Compliance Checks • NPC Circular 18-03 – Rules on Mediation before the National Privacy Commission 4.	Considerations: • Increased priority for cybersecurity. In 2018, Vietnam enacted the Law on Cybersecurity (24/2018/QH14), which increases the power granted to the State to investigate users and censor content published online by individuals. • Data localisation. The NIS Law establishes stricter requirements for foreign service providers operating in Vietnam, including data localisation in certain circumstances. Businesses that collect and process the personal data of Vietnamese citizens are required to maintain a physical office and store the data in Vietnam. Data protection rules can also be found in the following sectoral laws, as amended: • Decree on E-commerce (52/2013/ND-CP). Organisations and individuals conducting part or the whole of the process of commercial activity by electronic means connected to the internet, mobile telecommunications network or other open networks • Law on CyberSecurity (24/2018/QH14). Vietnamese and foreign enterprises which provide services on telecom networks and on the internet and other value added services in cyberspace, in Vietnam • Law on Information Technology (67/2006/QH11). Vietnamese and foreign organisations and individuals engaged in information technology application and development activities in Vietnam. 5. Law on Network Information Security (86/2015/QH13). Any Vietnamese agencies organisation, individual; foreign organisation and individual in Vietnam who directly involves in or is related to network information security activities in Vietnam.	Some other laws are restricting personal data sharing with external third parties without consent. (e.g. Employment security law: 6. http://www.japaneseelawtranslation.go.jp/la/w/detail_main?id=10&vm=&re=)	None	None	None	None found. The New Zealand Privacy Act 2020 will most likely be passed by its parliament later in 2020, and will amend the Privacy Act 1993. However, the proposed amendments do not present rules that duplicate or conflict with present legislation.