REFERENCE GUIDE TO PERSONAL DATA PRIVACY LAWS IN ASIA PACIFIC

		COLLECTION							USE AND DISCLOSURE						!	SECURITY				INDIVIDUAL RIGHTS					DATA EXPORTS					DATA PROCESSING					SPECIAL PROVISIONS														
	Collect minimum data necessary for purpose	Notice on collection from data subject	Notice on collection from third party	מו בטוופברווטוו	Notice can be given before, at or ASAP after collection	Collection requires consent	Collection must be rail and lawful	Anonymity if possible	Publish a privacy policy	Processing must be rair and tawful	Can be used/disclosed for related/compatible purposes	Can be used/disclosed as required or permitted by law	Can be used/disclosed as required or permitted by law	Can be used/disclosed with consent		uracy req	security r	preaches to auth	Disht to account and all all all all all all all all all al	Right to access personal data	Right to know disclosures to third parties	Right to correct personal data	Corrections must be advised to third parties	Right to delete personal data	Right to block use of personal data	Rights on sale of business	Delete / de-identify personal data after use completed	Restrictions on data exports across borders	Notice to data subject required	Permitted to white list countries specified by regulator	Permitted with consent of individual	Permitted with contract with receiving entity	Regulator has discretion to prohibit transfers	visions concernir	liable for own	due ditigence required of	nas obtigations regardir	Controller vicariously liable for processor	Direct marketing	Sensitive data	Record keeping requirements	Prior checking of some systems	Automated decisions	Data matching	Bublic registers	Public registers Visual surveillance	Visual surveillance	LEGISLATION	RESPONSIBLE AUTHORITY
*** Australia	•	•	• >	•	•	×	•	•	•	×	•	•	•	•	×	•	•	•	•	•	×	•	•	x :	×	×	•	•	•	×	•	•	×	×	Not a	ppli	icabl	le	•	•	×	×	×	×	,	x x	× Pr	rivacy Act 1988	Office of the Australian Information Commissioner
New Zealand	•	•	×	•	•	×	•	×	x :	x d	•	•	•	•	×	•	•	x :	×	•	×	•	•	x :	× :	×	•	•	×	×	×	×	•	•	•	c s	×	•	×	×	×	×	×	×	,	x x	× Pr	rivacy Act 1993	Office of the Privacy Commissioner
*** China	•	•	×		×	•	• :	×	•	• 3	(x	•	•	•	x :	x (•	•	• 3	x :	×	•	×	• :	x :	×	×	×	No	ot ap	oplic	able		×	Not a	ppli	icabl	le	•	x :	×	×	×	×	k	x x	× <u>De</u>	ecision of the NPC Standing Committee	Ministry of Industry and Information Technology
* Macau	•	•	×	• ;	x :	×	•	×	•	•	•	•	•	•	•	•	•	x :	×	•	×	•	• :	×	•	×	•	•	×	•	•	×	×	•	•	٠ (•	•	•	•	×	•	•	• ,	()	× •	• <u>Pe</u>	ersonal Data Protection Act 2006	Office for Personal Data Protection
* Hong Kong	•	•	×	• ;	x :	×	•	×	•	x d	•	•	•	•	•	•	•	x :	×	•	×	•	• :	x :	× :	×	•	×	No	ot ap	oplic	able	:	•	×	(•	•	•	x :	×	•	×	• •	•	×	х <u>Ре</u>	ersonal Data (Privacy) Ordinance 1996	Privacy Commissioner for Personal Data
Japan	×	•	•	• :	x :	×	•	x 3	x :	x d	•		•	•	×	•	• :	x :	×	• :	×	•	×	•	•	×	•	•	×	•	•	•	×	•	•	(•	x :	×	•	•	×	×	×	()	x x	× Ac	ct on the Protection of Personal formation 2003	Personal Information Protection Commission
Malaysia	×	•	•	• :	x :	x s	x :	x :	×	•	×	•	•	•	×	•	•	x :	×	• :	×	•	x :	×	•	×	•	•	×	•	•	•	×	•	×	,	x :	×	•	•	×	•	×	×	k s	x x	х <u>Ре</u>	ersonal Data Protection Act 2010	Department of Personal Data Protection
Philippines	×	•	×	•	•	•	• :	x 3	×	•	•		•	•	•	•	•	•	•		•	•	•	•	•	×	•	×	No	ot ap	oplic	able		•	•	,	x :	x :	×	•	×	×	•	×	k	x x	× <u>Da</u>	ata Privacy Act 2012	Department of Personal Data Protection
Singapore	•	•	×		x :	×	• :	×	• :	x	•		•	•	×	•	• :	x :	×	•	•	•	• :	x :	x	×	•	•	•	×	•	•	×	•	×	•	•	• :	x	x	×	×	×	×	k	x x	х <u>Ре</u>	ersonal Data Protection Act 2012	Personal Data Protection Commission
South Korea	•	•	•	•	×	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	×	•	•	•	•	•	•	×	•	×	×	•	•		•	•	•	•	×	•	×	×	,	x e	• <u>Pe</u>	ersonal Information Protection Act 2011	Personal Information Protection Commission
Taiwan	•	•	•	• :	x :	×	•	×	×	•	×	•	•	•	×	•	• :	x	•	•	×	•	•	•	•	×	•	•	×	×	×	×	•	•	•		•	•	•	•	×	×	×	×	k	x x	х Ре	ersonal Information Protection Act 2010	Ministry of Justice

Notes to table: 1. This table gives a simple "yes or no" indication of whether the relevant general principle is reflected in the selected countries' national private-sector data privacy laws. Industry-specific and sub-national laws are not considered. Every country's law is drafted differently and may reflect the principle in different terms. A principle may be marked "yes" despite being subject to exceptions and exemptions; a principle may be marked "no" because it is only partially or uncertainly reflected in the relevant law. 2. Hyperlinks are to English versions of legislation, which in some countries may be unofficial translations. 3. The information contained in this table is for general information purposes and are not intended to constitute legal advice. Concept adapted from Prof G Greenleaf, Asian Data Privacy Laws (2014). 4.Information up to date as of June 2018.

KEY FEATURES OF PERSONAL DATA PRIVACY LAWS IN ASIA PACIFIC

	Does the jurisdiction have a national personal data privacy law? Most jurisdictions also have narrower public-sector or industry-specific laws	Does the jurisdiction impose restrictions on transferring personal data overseas? Not including restrictions on disclosure to a third party generally, which also apply if the transfer is to an overseas third party	Does the jurisdiction mandate that security breaches affecting personal data must be notified to authorities or affected individuals?	Maximum fines for contravention Approximate USD conversions	Responsible authority
Australia	Privacy Act 1988	Yes, may only transfer to a country with a similar level of privacy protection, with consent of individual or in certain other circumstances: Australian Privacy Principle 9.	Yes, an organisation is required to notify the regulator and affected individuals of any data breach involving personal information, if serious harm may result: Part IIIC.	Up to AU\$1,700,000 (US\$1,350,000).	Office of the Australian Information Commissioner
New Zealand	Privacy Act 1993	No. The Privacy Commissioner has the discretion to issue a transfer prohibition notice, but has never exercised this power.	No.	Up to NZ\$2,000 (US\$1,500).	Office of the Privacy Commissioner
** China	The <u>Decision of the Standing Committee of the National People's Congress on Strengthening the Network Information Protection</u> (the <u>Decision</u>) is the leading data privacy legislation but sets out general data privacy principles only. The <u>Cybersecurity Law</u> and the <u>Law on the Protection of Consumer Rights and Interests</u> provide further industry-specific rules. The <u>Guidelines for Personal Information Protection for Information Systems in Public and Commercial Services</u> (the <u>Guidelines</u>) are more detailed, but voluntary.	The voluntary <i>Guidelines</i> provide that personal information may only be transferred overseas with the express consent of the data subject, the consent of the relevant authorities, or express legal or regulatory permission: article 12. The <i>Cybersecurity Law</i> imposes restrictions on data exports, but only by providers of "critical information infrastructure": article 37. Also consider the restrictions of the <i>State Secrets Law</i> .	Network operators must report breaches to authorities under clause V of the <i>Decision</i> . They are also required to notify affected individuals under article 42 of the <i>Cybersecurity Law</i> .	Breach of the <i>Decision</i> - unspecified fines and confiscation of profits. Breach of the <i>Cybersecurity Law</i> - up to RMB1,000,000 (US\$150,000). Breach of the <i>Consumer Law</i> - up to RMB500,000 (\$75,000).	Ministry of Industry and Information Technology
<u>∗</u> Macau	Personal Data Protection Act 2006	Yes, all overseas transfers must either be notified to or authorised by the Office for Personal Data Protection, depending on the circumstances: articles 19-20.	No.	Up to MOP\$200,000 (US\$24,500).	Office for Personal Data Protection
★ Hong Kong	Personal Data (Privacy) Ordinance 1996	No, relevant section of the <i>Personal Data (Privacy) Ordinance</i> is yet to be enacted. May be enacted in next year or two.	No.	Up to HK\$1,000,000 (US\$128,000).	Privacy Commissioner for Personal Data
Japan	Act on the Protection of Personal <u>Information 2003</u>	Yes, may only transfer to a country which the regulator has recognised as adequate, with the consent of the individual, or if the recipient has established a compliant system for protecting personal data: article 24.	No, but the relevant authority can order a business to make a report on a breach: article 40.	Up to JPY500,000 (US\$4,500).	Personal Information Protection Commission
Malaysia	Personal Data Protection Act 2010	Yes, may only transfer to a country with a similar level of privacy protection, with consent of individual or in certain other circumstances: section 129.	No.	Up to MYR\$500k (US\$120,000).	Department of Personal Data Protection
Philippines	Data Privacy Act 2012	No. A data controller will remain "accountable" for compliance with the Act when data is disclosed to overseas third parties (section 21) but it is uncertain whether the controller would be legally liable if the Act was breached by that third party.	Yes, for a data breach involving sensitive personal information or information that may be used to facilitate identity fraud, if there is a real risk of serious harm to an individual as a result of the breach: section 20(f).	Up to PH₱5,000,000 (US\$97,000).	National Privacy Commission
Singapore	Personal Data Protection Act 2012	Yes, may only transfer to a country with a similar level of privacy protection, with consent of individual or in certain other circumstances: section 26(1). An organisation may apply to the Commission to be exempted from these restrictions.	Under section 14 of Singapore's new <u>Cybersecurity Act 2018</u> (which will take effect in 2018), entities operating 'critical information infrastructure' are required to report certain cybersecurity incidents to the Commissioner of Cybersecurity.	Up to SG\$1,000,000 (US\$740,000).	Personal Data Protection Commission
South Korea	Personal Information Protection Act 2011	Yes, consent must be obtained from the individual: article 17.	Yes, it must notify the data subject, and for large breaches, the Ministry of Security and Public Administration or other authorities: article 34.	Up to KR₩50m (US\$44,000).	Personal Information Protection Commission
Taiwan	Personal Information Protection Act 2010	No. The government has a discretion to prohibit the transfer of personal data to countries with inadequate privacy protection, but it has rarely exercised this discretion: article 21.	Yes, if an entity breaches the Act and as a result personal information is stolen, disclosed, altered or infringed, the entity must notify affected individuals: article 12. No requirement to notify government.	Up to TW\$1,000,000 (US\$33,000).	Ministry of Justice
Thailand	No. Industry-specific laws exist covering telecommunications and banking. The government is drafting a <u>Personal Data Protection Act.</u>	No.	No.	Not applicable.	No privacy regulator
Indonesia	No. However, the <u>Electronic Information and Transaction Law</u> (EIT Law) contains provisions relating to electronic data only.	No.	An electronic system operator is required under the <i>EIT Law</i> to notify affected individuals of a security breach.	Up to IDRp12bn (US\$890,000).	Ministry for Communications and Informatics
• India	Not in practice. A set of Rules made under the <u>Information Technology Act 2000</u> resemble a data privacy law, but they may be <u>ultra vires</u> , apply only to "sensitive personal data" and are not enforced.	Not in practice. Rule 7 sets out restrictions on data export, but the rule only applies to sensitive personal data, is ambiguous and is not enforced.	No.	Up to IN₹500k (US\$8,000).	Department of Electronics and Information Technology
★ Vietnam	No. However, the <u>Law on Network Information Security</u> contains some basic provisions on the collection and handling of personal information.	No.	No.	Up to VND70,000,000 (US\$3,000).	No privacy regulator

Hyperlinks are to English versions of legislation, which in some countries may be unofficial translations. This information is up to date as of June 2018. It is for general information purposes and is not intended to constitute legal advice.

