
















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 Decision of the Standing Committee of the National People's Congress on Strengthening the Network Information Protection (the <i>Decision</i>) is the leading data privacy legislation but sets out general data privacy principles only. The Cybersecurity Law and the Law on the Protection of Consumer Rights and Interests provide further industry-specific rules. The Guidelines for Personal Information Protection for Information Systems in Public and Commercial Services (the <i>Guidelines</i>) 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
 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 Information 2003	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 PHP5,000,000 (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 Cybersecurity Act 2018 (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 S\$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 Personal Data Protection Act .	No.	No.	Not applicable.	No privacy regulator
 Indonesia	No. However, the Electronic Information and Transaction Law (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 Information Technology Act 2000 resemble a data privacy law, but they may be <i>ultra vires</i> , 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 Law on Network Information Security 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.