



**| International
Privacy Checklist**

LexisNexis® Regulatory Compliance

LexisNexis Regulatory Compliance is a legal obligations register and alerting solution that combines regulatory content with technology to empower you to take control of your compliance obligations.

About the International Privacy Modules

LexisNexis Regulatory Compliance Privacy modules guides your organisation through the complex compliance obligations surrounding the collection, management and maintenance of personal information. Our Privacy modules cover multiple jurisdictions including Australia, New Zealand, US, UK, Japan, Singapore, China and Hong Kong.

About the Expert

Dudley Kneller,
Partner, Gadens



Dudley is a highly experienced lawyer with international and domestic experience advising on commercial, regulatory and technology matters with specialisations in financial technology, cyber risk, privacy and strategic sourcing and supply projects.

Dudley has over 20 years' experience practising across Australia, Europe and the UK, and has worked on projects based in a range of countries, including the Philippines, India and across South America.

Dudley publishes and presents extensively. He has been nominated and selected as a 'Best Lawyer' in Australia in the area of Information Technology Law since 2020 and has been listed as a Recommended Technology, Media and Telecommunications Lawyer in Victoria in Doyle's Guide every year from 2015 to 2020.

INTERNATIONAL PRIVACY CHECKLIST

This checklist has been designed to help you identify your international privacy requirements when handling personal information.

Applicability of Privacy Laws

Requirement	Don't know	Not yet	Yes
Can the organisation identify which information is subject to privacy laws?			
Can the organisation identify which information is subject to enhanced protections under privacy laws (for example health information, sensitive information)?			
Can the organisation identify which jurisdiction governs the information it collects?			
Can the organisation identify any circumstances where privacy laws will not apply?			

Organisational Governance

Requirement	Don't know	Not yet	Yes
Does the organisation publish a privacy policy that details its information handling procedures, the rights of consumers and a complaints process?			
Does the organisation have a privacy officer responsible for ensuring compliance with all applicable privacy legislation?			
Does the organisation empower the privacy officer to cooperate with authorities during investigative and enforcement actions?			
Does the organisation have a privacy program designed to promote a culture of information privacy compliance?			
Does the organisation keep all prescribed records and any additional records necessary to demonstrate compliance?			

Collecting Personal Information

Requirement	Don't know	Not yet	Yes
Does the organisation only collect personal information for a clearly stated and lawful purpose?			
Does the organisation collect personal information directly from individuals whenever possible?			
Does the organisation inform individuals of the purpose of collecting their personal information before collecting the information?			
Does the organisation notify individuals that their information has been collected?			
Does the organisation inform individuals of the likely recipients of information disclosures (and the geographic location of likely recipients)?			
Does the organisation destroy collected personal information unless it has a lawful reason for retention?			
Does the organisation permit individuals to provide their information anonymously if practicable?			

Ensuring the Accuracy of Personal Information

Requirement	Don't know	Not yet	Yes
Does the organisation take reasonable steps to verify the accuracy of personal information before use?			
Does the organisation make requested corrections to personal information when the correction will improve accuracy?			
Does the organisation systematically update stored information to ensure accuracy over time?			

Using and Disclosing Personal Information

Requirement	Don't know	Not yet	Yes
Does the organisation only use and disclose personal information in accordance with all applicable privacy laws?			
Does the organisation only use and disclose personal information for the purpose stated at collection or a related purpose?			
Does the organisation obtain consent from individuals before using or disclosing their personal information for new purposes?			
Has the organisation defined the emergency circumstances that will enable use and disclosure of personal information without consent?			
Does the organisation obtain explicit consent from individuals before using or disclosing their personal information for marketing purposes?			
Does the organisation enable individuals to opt out of direct marketing activities?			
Does the organisation enable individuals to block uses and disclosures of their personal information?			

Ensuring the Security of Personal Information

Requirement	Don't know	Not yet	Yes
Does the organisation take every reasonable step to protect stored personal information from loss, interference or unauthorised disclosure?			
Does the organisation tailor and apply security controls to stored personal information that are proportionate to the sensitivity of the information?			
Does the organisation identify and flag sensitive and confidential information subject to enhanced privacy rules?			
If the organisation is large or collects highly sensitive information, does it perform routine data security audits?			
Does the organisation have an incident response plan containing appropriate measures to limit the damage caused by a data breach?			
Does the organisation assign responsibility for information security to an appropriate individual or team?			
Does the organisation notify affected individuals after a data breach?			
Does the organisation notify authorities after a data breach?			
Does the organisation destroy stored information securely?			

Enabling Access to Personal Data and Correction of Personal Data

Requirement	Don't know	Not yet	Yes
Does the organisation enable individuals to view their personal information within a reasonable timeframe?			
Does the organisation only refuse to provide individuals with access to their personal information for appropriate reasons?			
Does the organisation inform individuals who view their personal information that they are entitled to make a correction?			
Does the organisation make all requested changes to stored personal information unless the request will reduce the accuracy of the information?			
Does the organisation attach a statement of correction to stored personal information on request?			
Does the organisation delete the personal information of individuals on request?			
Does the organisation only charge individuals to access, correct or delete their personal information as allowed by applicable privacy laws?			
Is the organisation prepared to cooperate with privacy reviews conducted by authorities?			







Overseas Transfers of Information


Requirement	Don't know	Not yet	Yes
Does the organisation maintain awareness of the current restrictions that apply to overseas transfers of data in all relevant jurisdictions (for example under privacy principles or adequacy decisions)?			
Does the organisation obtain express consent from individuals before transferring their personal information overseas?			
Does the organisation only transfer personal information to overseas recipients that are subject to comparable enforceable privacy standards?			
Does the organisation only import personal information in compliance with the privacy regime of the country of origin?			
Does the organisation maintain awareness of prohibitions on overseas information transfers imposed by authorities?			


Privacy Complaints and Investigations

Requirement	Don't know	Not yet	Yes
Does the organisation maintain formal processes for receiving, assessing and responding to privacy complaints?			
Does the organisation assign responsibility for handling and responding to complaints to an appropriate officer or team?			
Is the organisation prepared to cooperate with privacy complaint investigations conducted by external authorities?			
Does the organisation maintain the management systems necessary to receive and comply with enforcement instruments at short notice?			

FEATURES

	What national law governs the privacy of personal information?	Which entities are subject to the national privacy law?	What information is subject to the national privacy law?	What restrictions apply to overseas transfers of data?	Who is the responsible authority?	What is the maximum penalty for breaching the national privacy law?	Notes
 Australia	Privacy Act 1988 (Cth)	Public agencies, organisations with annual turnover greater than A\$3,000,000	Any information about an individual that can be connected to that individual	Overseas recipients must be bound to comparable privacy rules by law or contract provisions.	Office of the Australian Information Commissioner	A\$444,000 (individuals) and A\$2,220,000 (corporations) for serious and repeated breaches	Larger penalties apply under the Competition and Consumer Act, such as for breaches of consumer data rights provisions.
 NZ	Privacy Act 2020 (NZ)	All individuals, organisations and public agencies	Any information about an individual that can be connected to that individual	Entities must ensure overseas recipients are bound by comparable privacy standards.	Office of the Privacy Commissioner	NZ\$10,000 for offences against the Privacy Act	The OPC can also make an official complaint to the Human Rights Tribunal, which can award damages of up to NZ\$350,000.
 Singapore	Personal Data Protection Act 2012 (SNG)	Private sector organisations only, excluding organisations handling data on behalf of a public agency	Any information that can be connected to an individual alone or in combination with other held data	Entities must obtain consent and ensure overseas recipients are bound by comparable privacy standards.	Personal Data Protection Commission	SG\$1,000,000 or 5% of a large company's annual turnover for failing to prevent privacy breaches	Personal Data Protection (Amendment) Act 2020 (SNG) partially commenced 1 February 2021.
 Japan	Act on the Protection of Personal Information 2003 (JPN)	All organisations and public agencies	Any information that can be connected to a living individual alone or in combination with other held data	Transfers only with consent, or to countries approved by the commission, or with approved assurances.	Personal Information Protection Commission	¥500,000 and 1 year imprisonment with work for misusing personal information for profit	New amendments will take effect before June 2022.
 China	Cybersecurity Law 2016 (CHN)	All organisations that collect electronic information from individuals in mainland China	Any information that can be used to identify an individual alone or in combination with other held data	Critical information infrastructure operators should only transfer if necessary and after a security assessment. Voluntary guidelines recommend obtaining consent from data subjects.	Ministry of Industry and Information Technology of the People's Republic of China	Unspecified fines, confiscation of income, cancellation of permits, closure of services and work bans	Draft of the Personal Information Protection Law released for consultation on 21 October.
 Hong Kong	Personal Data (Privacy) Ordinance (HK)	All individuals, organisations and public agencies	Any information about a living individual that can be connected to that individual	N/A	Office of the Privacy Commissioner for Personal Data	HK\$1,000,000 and 5 years imprisonment for selling information for direct marketing purposes	Overseas data transfer rules present in PDPO but never enacted.

 UK	<p>Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (UK)</p> <p>Data Protection Act 2018 (UK)</p> <p>General Data Protection Regulation (GDPR) (EU)</p>	<p>All individuals, organisations and public agencies</p>	<p>Any information relating to an individual that can be connected to that individual</p>	<p>Transfers only with consent, or to whitelisted recipients, or with approved assurances.</p>	<p>The Information Commissioner's Office</p>	<p>€20,000,000 or 4% of worldwide turnover for breaching UK GDPR privacy principles</p>	<p>The DPPEC Regulation preserves all the data protection standards previously under the EU GDPR. The EU GDPR may also apply depending on an organisation's activities and locations.</p>
--	---	---	---	--	--	---	---

 USA (Cali)	<p>None - the California Consumer Privacy Act (Cal. Civ. Code § 1798:100 et seq.) represents best practice</p>	<p>The CCPA applies to organisations with at least US\$25m in revenue or that handle large amounts of personal data</p>	<p>The CCPA covers any information collected from an individual that can be connected to that individual</p>	<p>N/A</p>	<p>The California Attorney General enforces the CCPA</p>	<p>US\$7,500 per violation of the CCPA</p>	<p>The CCPA is enforceable only in California - other states enforce alternative privacy regimes.</p>
--	--	---	--	------------	--	--	---

About LexisNexis® Regulatory Compliance

LexisNexis Regulatory Compliance is a legal obligations register and alerting solution that combines regulatory content with technology to empower you to take control of your compliance obligations.

We use Australia's leading legal and industry experts to provide a practical, plain English interpretation of all the relevant legislative and regulatory materials, so you don't have to.

Content is updated regularly, so you can access obligations which reflect the current legislative framework - saving you significant costs and / or research time.

All content is supported with flexible technology options designed to meet your existing and future needs.

LexisNexis Regulatory Compliance makes your compliance journey fast and seamless.

About LexisNexis

LexisNexis is part of RELX Group, a world-leading provider of information and analytics for professional and business customers across industries. LexisNexis helps customers to achieve their goals in more than 175 countries, across six continents, with over 10,000 employees.