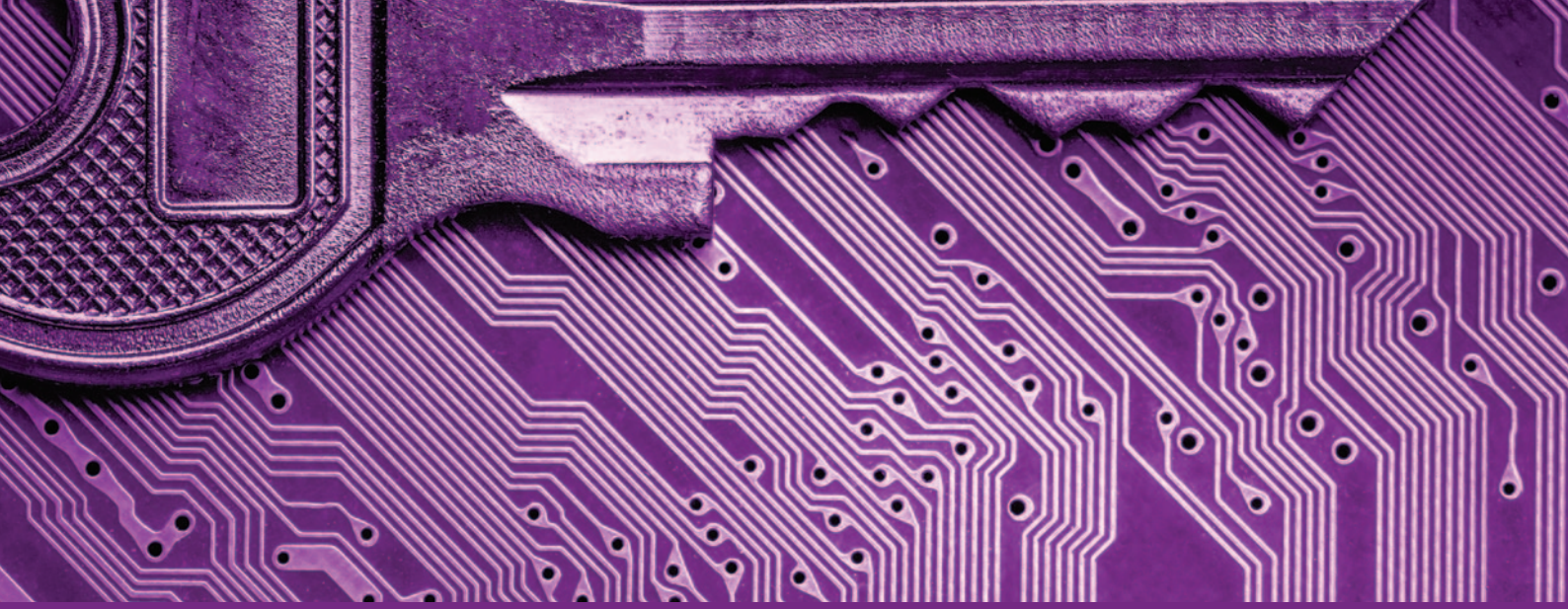

ICLG

The International Comparative Legal Guide to:

Data Protection 2019

6th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Addison Bright Sloane
Anderson Mōri & Tomotsune
Ashurst Hong Kong
Assegaf Hamzah & Partners
BEITEN BURKHARDT
Bird & Bird
Christopher & Lee Ong
Çiğdemtekin Çakırca Arancı Law Firm
Clyde & Co
Cuatrecasas
Deloitte Legal Shpk
DQ Advocates Limited
Drew & Napier LLC
Ecija Abogados
FABIAN PRIVACY LEGAL GmbH
GANADO Advocates
Herbst Kinsky Rechtsanwälte GmbH
Herzog Fox & Neeman
Infusion Lawyers
Integra Law Firm
KADRI LEGAL
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys At Law
Lee & Ko
LPS L@w
Lydian
Matheson
Mori Hamada & Matsumoto
Morri Rossetti e Associati Studio Legale e Tributario
Nyman Gibson Miralis
OLIVARES
Osler, Hoskin & Harcourt LLP
Pestalozzi Attorneys at Law
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Rothwell Figg
S. U. Khan Associates Corporate & Legal Consultants
Subramaniam & Associates (SNA)
thg IP/ICT
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg global legal group

global legal group

Contributing Editor
Tim Hickman &
Dr. Detlev Gabel,
White & Case LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Nicholas Catlin

Senior Editors
Caroline Collingwood
Rachel Williams

CEO
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
June 2019

ISBN 978-1-912509-76-8
ISSN 2054-3786

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Continued Overleaf

global legal group

Country Question and Answer Chapters:

Chapter 6

Australia

Dennis Miralis

Phillip Gibson

Nyman Gibson Miralis

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The *Privacy Act 1988* (Cth) ('**Privacy Act**'), including the Australian Privacy Principles ('**APPs**').

1.2 Is there any other general legislation that impacts data protection?

The *Do Not Call Register Act 2006* (Cth) ('**DNCRA**') and *Spam Act 2003* (Cth) ('**Spam Act**') set out limits to direct marketing activities.

At the state and territory level, there is much legislation concerned with data protection including, for example: the *Information Privacy Act 2014* (ACT), the *Privacy and Personal Information Protection Act 1998* (NSW), the *Information Privacy Act 2009* (Qld), the *Personal Information and Protection Act 2004* (Tas), and the *Privacy and Data Protection Act 2014* (Vic).

1.3 Is there any sector-specific legislation that impacts data protection?

Privacy issues specific to the telecommunications sector are contained within the *Telecommunications Act 1997* (Cth) ('**Telecommunications Act**') and the *Telecommunications (Interception and Access) Act 1979* (Cth).

Information related to healthcare is further protected under the *My Health Records Act 2012* (Cth) and the *Healthcare Identifiers Act 2010* (Cth). A multiplicity of state legislation also exists in relation to the protection of health-based privacy.

Businesses in industries such as financial services and gambling must comply with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and *Anti-Money Laundering and Counter-Terrorism Financing Rules*.

1.4 What authority(ies) are responsible for data protection?

The Office of the Australian Information Commissioner ('**OAIC**') is an independent statutory agency which is endowed with functions under the Privacy Act and other legislation relating to data protection.

The Australian Communications and Media Authority ('**ACMA**') is the regulatory authority charged with enforcing the DNCRA and Spam Act, as well as having other functions under the Telecommunications Act.

The Commonwealth Attorney-General's Department has responsibilities under the *Telecommunications (Interception and Access) Act*.

In coordination with the OAIC, the National Health and Medical Research Council has issued a number of binding guidelines in respect of privacy concerning health-related information.

The Australian Transaction Reports and Analysis Centre ('**AUSTRAC**') is the agency responsible for administering the *Anti-Money Laundering and Counter-Terrorism Financing Act*.

Various state and territory authorities also regulate privacy law issues in those jurisdictions. These include: the ACT Information Privacy Commissioner; the New South Wales Information and Privacy Commission; the Office of the Information Commissioner for the Northern Territory; the Queensland Office of the Information Commissioner; the South Australian Privacy Committee; the Tasmanian Ombudsman; the Office of the Victorian Information Commissioner; and the Office of the Information Commissioner for Western Australia.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"

  The analogous term used in the Privacy Act is 'personal information'. This is defined in section 6 of the Privacy Act to mean information or an opinion about an identified individual, or an individual who is reasonably identifiable:

  a) whether the information or opinion is true or not; and

  b) whether the information or opinion is recorded in a material form or not.

- "**Processing**"

  The Privacy Act does not refer to 'processing', but regulates 'dealing with' personal information in terms of 'use' and 'disclosure' (see Part 3 of the APPs). Though both terms are not defined in the Privacy Act, the OAIC indicates that:

  - 'Use' means the handling or undertaking of activity in respect of information within its effective control.
  - 'Disclose' means to make information accessible to others outside the entity and to release subsequent handling of such information from the entity's control.

- "**Controller**"

  The Privacy Act does not refer to 'controllers' but rather covers the information-processing activities of APP entities. APP entities include agencies and organisations. Agencies include:

  - government ministers or departments;
  - bodies established for a public purpose;
  - bodies established by the Governor-General or a Minister;
  - a person holding an office by appointment under an Act or by the Governor-General;
  - a federal court; or
  - the Australian Federal Police.

  Organisations include:

  - individuals;
  - bodies corporate;
  - partnerships;
  - other unincorporated associations; and
  - trusts.

  Organisations do not include small business operators, registered political parties, agencies, or State and Territory authorities.

- "**Processor**"

  Whilst the term 'processor' is not used in the Privacy Act, the APPs naturally apply to APP entities to the extent that they hold personal information. According to the OAIC, this is sufficiently broad to encompass outsourced serviced providers which, for example, in Europe might be considered 'processors'.

- "**Data Subject**"

  The Privacy Act regulates the processing of personal information about individuals, defined in section 6 to mean natural persons.

- "**Sensitive Personal Data**"

  'Sensitive information' is defined by section 6 of the Privacy Act to mean:

  a) Personal information about an individual's:
     i. racial or ethnic origin;
     ii. political opinions;
     iii. membership of a political association;
     iv. religious beliefs or affiliations;
     v. philosophical beliefs;
     vi. membership of a professional trade association;
     vii. membership of a trade union;
     viii. sexual orientation or practices; or
     ix. criminal record;
  b) health information;
  c) genetic information;
  d) biometric information; or
  e) biometric templates.

- "**Data Breach**"

  'Eligible data breach' is defined by section 26WE(2) of the Privacy Act as occurring where:

  - there is unauthorised access to, or disclosure of, information (or it is lost in circumstances where such access or disclosure is likely to occur); and
  - a reasonable person would conclude such access or disclosure would be likely to result in serious harm to any individual to which the information relates.

Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data").

- "**Collects**"

  As defined in section 6 of the Privacy Act, an entity collects personal information only if this is done for inclusion in a record or generally available publication.

- "**De-identified**"

  Personal information is de-identified if it is no longer about an identified individual or an individual who is reasonably identifiable.

- "**Employee record**"

  This means a record of personal information relating to the employment of an employee, including their health, resignation/termination, contact details, salary/wages, union/professional association membership, and taxation affairs.

- "**Holds**"

  An entity holds personal information if it possesses or controls a record that contains such information.

- "**Identification information**"

  Identification information about an individual means the person's:

  - full name;
  - alias or previous name;
  - date of birth;
  - sex;
  - current or last known address and two previous addresses;
  - current or last known employer; or
  - driver's licence number.

- "**Record**"

  A record includes a document or electronic or other device. It does not, however, include:

  - generally available public information;
  - anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition;
  - Commonwealth records in the open access period;
  - records in the care of the National Archives of Australia;
  - documents placed in the memorial collection of the Australian War Memorial; or
  - letters or articles transmitted by post.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Section 5B(1A) of the Privacy Act extends its application to acts done outside Australia by an organisation, or small business operator, with an Australian link. For businesses established outside Australia, an Australian link could cover situations where business is carried on in Australia and the personal information was collected or held in Australia. However, section 6A of the Privacy Act dictates that the APPs will not be breached by any conduct external to Australia that is required by an applicable foreign law.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  APP 1 aims to ensure that personal information is managed in an open and transparent way. Entities are required to implement practices, procedures and systems to comply with the APPs and enable them to deal with enquiries/complaints in this regard. It also necessitates a clearly expressed privacy policy that is freely available.

- **Lawful basis for processing**

  Broadly speaking, the lawful basis upon which an entity may process personal data is the consent of the individual. However, the majority of the APPs contain limitations or extensions relating to the application of Commonwealth laws, records, and/or agreements. APP 3.5 specifies that personal information may only be collected by lawful and fair means.

- **Purpose limitation**

  Pursuant to APP 6, where an entity has collected personal information for a particular person, that information cannot then be used or disclosed for any further purpose other than with consent of the individual. This is limited, however, by certain defined exceptions, such as where the individual would hold a reasonable expectation of disclosure, where disclosure is required/authorised by a court or tribunal, or where a certain permitted health situation exists (See APPs 6.2 and 6.3).

- **Data minimisation**

  The APPs address data minimisation in a piecemeal approach, combining a prohibition on reallocation of the purpose for holding information without consent (APP 6), limiting the collection of information to that which is reasonably necessary for the function in question (APP 3), and mandating destruction/de-identification where no purpose for use or disclosure of the information remains (APP 11).

- **Proportionality**

  Pursuant to APP 3, an APP entity may only collect personal information to the extent that it is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. For sensitive information, collection further requires the individual's consent.

- **Retention**

  When an entity holds personal information, and no purpose for its use or disclosure remains, APP 11.2 requires the entity to destroy or de-identify the information. This does not apply to information on a Commonwealth record or required to be retained by law.

Other key principles – please specify

- **Collection of unsolicited personal information**

  Where an APP entity receives non-solicited personal information, APP 4 requires it to determine whether or not such information could have been solicited under APP 3. If this could not have been done (subject to certain limitations), the entity must destroy the information or ensure its de-identification.

- **Cross-border disclosure**

  Unless authorised, entities that intend to disclose personal information in a cross-border context must, pursuant to APP 8, take reasonable steps to ensure that the foreign entity receiving such information complies with the APPs. This is subject to exceptions, such as where that foreign entity is subject to a similar privacy regime under foreign law, or the information is being disclosed pursuant to a treaty obligation.

- **Government-related identifiers**

  APP 9 prohibits (with certain exceptions) the adoption, use or disclosure of government-related identifiers for individuals, by non-government organisations.

- **Quality of personal information**

  APP 10 mandates that personal information held, used, and disclosed should be accurate, up-to-date, and complete.

- **Security**

  Where an APP entity holds personal information, APP 11 dictates that it must take reasonable steps to protect this from misuse, interference, loss and unauthorised access, modification or disclosure.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**

  Upon request from the concerned individual, an entity holding personal information must give that individual access to such information. This does not apply where information is held by a government agency that has a lawful reason for non-disclosure, or in certain circumstances such as where access would pose a serious threat to health or safety or would unreasonably impact the privacy of others.

- **Right to rectification of errors**

  APP 10 mandates that personal information held, used, and disclosed should be accurate, up-to-date, and complete. Pursuant to APP 13, upon request by an individual, an entity must take reasonable steps to correct any of that person's information that is inaccurate, out-of-date, incomplete, irrelevant, or misleading.

- **Right to deletion/right to be forgotten**

  APP 11.2 requires that reasonable steps be taken to delete or de-identify personal information once its purpose/s for use no longer exists. This is subject to the information not being in a Commonwealth record and the APP entity not being required by law to retain the information. Despite some discussion about legislative reform in this area, however, there is no right to be forgotten under Australian law, similar to the right under European law.

- **Right to object to processing**

  In practical terms, an individual's power to restrict processing of their personal information is limited to their initial withholding of consent to the collection of such information. APP 2 requires that persons be allowed not to identify themselves when dealing with an APP entity (unless required/permitted by law, or if this would be impractical). Additionally, APP 5 requires that individuals be notified before (or as soon as practicable after) their personal information is collected, thereby giving them the opportunity to object to such collection by disengaging with the entity.

- **Right to restrict processing**

  Whilst the APPs impose certain restrictions on how personal information can be dealt with (such as those relating to the purpose for which information is held (APPs 3 and 6)), there is no right bestowed on individuals to restrict the manner with which their information is dealt. Any such control held by an individual is largely relinquished upon the initial giving of consent to its collection.

- **Right to data portability**

  A broad right to data portability does not presently exist under Australian law (although, pursuant to APP 12, individuals can

request a copy of their personal information held by an APP entity). However, the Australian Government is actively moving to progressively legislate this right – to be known as 'consumer data right' ('**CDR**') – into Australian law. CDR will first apply to the banking sector, and will allow persons to request that their data be shared with an accredited recipient. The Australian Competition and Consumer Commission will be the lead regulator of CDR.

- **Right to withdraw consent**

  According to the OAIC, individuals should be provided with an easy and accessible process to withdraw their consent to the use or disclosure of their personal information. The withdrawal of consent invalidates formerly given consent being relied upon in relation to future use or disclosure of that person's information. However, individuals must be advised of the implications of their consent being withdrawn.

- **Right to object to marketing**

  APPs 7.2 and 7.3 require APP entities using personal information to engage in direct marketing to provide a simple means by which individuals may easily request to not receive such communications, which is drawn to the individual's attention. If such a request is made, the entity must cease direct marketing to the individual.

- **Right to complain to the relevant data protection authority(ies)**

  The OAIC is empowered to receive individual complaints about the handling of personal information. It can also recognise external dispute-resolution schemes ('**EDRS**') that handle particular privacy-related complaints. For example, from 1 November 2018 the Australian Financial Complaints Authority was recognised as an EDRS for the financial services industry.

Other key rights – please specify

- **Right to anonymity**

  Pursuant to APP 2, individuals must have the option of not identifying themselves or using a pseudonym when dealing with APP entities, unless that entity is required/authorised by law to deal with individuals who have identified themselves, or if dealing with non-identified individuals would be impracticable.

- **Right to notification**

  APP 5 mandates that individuals are notified of the collection of their personal information before, or as soon as practicable after, it occurs.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

There is no legal obligation on businesses to register with or notify the OAIC or any other bodies in relation to their data-processing activities in general. Specific obligations arise when eligible data breaches occur, as detailed in question 15. However, the OAIC has issued guidance to assist APP entities to prepare responses to any such breaches.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable in Australia – please see question 6.1.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable in Australia – please see question 6.1.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable in Australia – please see question 6.1.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable in Australia – please see question 6.1.

6.6 What are the sanctions for failure to register/notify where required?

This is not applicable in Australia – please see question 6.1.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable in Australia – please see question 6.1.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable in Australia – please see question 6.1.

6.9 Is any prior approval required from the data protection regulator?

This is not applicable in Australia – please see question 6.1.

6.10 Can the registration/notification be completed online?

This is not applicable in Australia – please see question 6.1.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable in Australia – please see question 6.1.

6.12 How long does a typical registration/notification process take?

This is not applicable in Australia – please see question 6.1.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Such an appointment is optional. The OAIC recommends that entities consider designating privacy officers that regularly report to their governance bodies as part of their obligations to implement practices, procedures and systems to ensure compliance with the APPs.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

This is not applicable in Australia – please see question 7.1.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

This is not applicable in Australia – please see question 7.1.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

In relation to government agencies, the OAIC recommends that privacy contact officers be of sufficient seniority to be involved in many aspects of the agency's operations, including its decision-making processes.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable in Australia – please see question 7.1.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The OAIC recommends that privacy officers regularly report to their entity's governance body. In relation to best practice for government agencies, the OAIC recommends that privacy contact officers should be at least at the executive level and:

- participate in the development of initiatives with a privacy impact;
- advise on the application of the Privacy Act;
- handle or supervise the handling of privacy complaints;
- train staff in relation to relevant aspects of the Privacy Act; and
- be the primary contact for the OAIC.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No, registration/notification is not required.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

No. The OAIC requires privacy policies to be high-level documents that are not expected to contain detail about all the entity's practices, procedures and systems relating to management of personal data.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

As the APPs do not specifically refer to 'processors', this is not strictly the case.

However, although the Privacy Act and APPs do not refer explicitly to processors, the OAIC's view is that APP entities which are outsourced service providers holding personal information, even if not controlling it as such, must comply with this legal regime.

Where the processor is located overseas, the regulation of foreign information transfer, as detailed below in question 8, will apply.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Although not applicable, entering such agreements remains best practice. In the context of cross-border disclosure, the OAIC recommends that such contracts cover:

- the type of personal information and purpose for its disclosure;
- a requirement that the recipient of the information complies with the APPs;
- the complaints-handling process; and
- a requirement as to the implementation of a data-breach response plan.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

APP 7.1 imposes a general prohibition on the use of personal information for the purpose of direct marketing. This does not apply where the organisation provides a simple means through which the individual can opt-out of the marketing and:

- the information was collected in circumstances that would give rise to reasonable expectation of the information being used in such marketing; or
- the individual has consented to the receipt of such marketing.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The DNCRA prohibits most unsolicited telemarketing calls and fax messages to numbers placed on a national Do Not Call Register, without the consent of the person/organisation being contacted.

The Spam Act proscribes the sending of most unsolicited and non-consensual electronic messages. Some exceptions to this prohibition are electronic messages by government bodies, political parties and charities.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The Spam Act regulates the sending of commercial electronic messages with 'an Australian link'. This covers messages that:

- originate in Australia;
- were sent, or authorised by, an individual/organisation physically present in Australia, or with central management and control in Australia, when the message was sent;
- were accessed by a computer, server or device that is located in Australia;
- is connected to an electronic account-holder that is either an individual physical present in Australia or an organisation carrying on business or activities in Australia when the message is accessed; or
- if unable to be delivered due to the non-existence of a delivery address would, had the address existed, reasonably likely have been accessed using a computer, server, or device located in Australia.

The DNCRA concerns telephone calls and fax messages sent to 'an Australian number'. This means numbers that are specified in the plan set out in the Telecommunications Act and for use in connection with the supply of carriage services to the public in Australia. Section 9 of the DNCRA also expressly extends the legislation's application to acts done outside Australia's territory.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. The ACMA, which is the regulatory authority charged with enforcing the DNCRA and Spam Act, regularly publishes its actions taken in discharging these functions.

For example, in February 2019 an e-marketing company was fined almost $40,000 for breaches of the Spam Act arising from third party marketing. Further, in January 2019 the ACMA penalised a telecommunications provider over $50,000 for making telemarketing calls to numbers on the Do Not Call Register.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Yes. However, when doing so, the purchaser must ensure their compliance with APP 7.3. This requires that persons have either consented to receipt of marketing or that it is impractical to obtain such consent and that in each communication recipients are provided, via a prominent statement, with a simple means to 'opt out' of these communications.

Under APP 7.6(e), individuals may request to be advised of the source of their personal information used or disclosed in relation to direct marketing.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Breaches of the DNCRA may result in corporate liability for civil penalties up to $2.1 million, and individual liability for up to $420,000 per day. This will depend on the number of breaches and history of the actor. Compensation can also be ordered where a victim has suffered loss or damage.

This penalty regime (and maximum sanctions) is largely mirrored in respect of the Spam Act.

Additionally, the Privacy Act contains numerous provisions addressing the payment of civil penalties, fines and compensation to victims.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no specific legal regime that applies to cookies. Whilst the information collected through the use of cookies is often generalised, where it rises to the level of enabling identification of an individual, the use of cookies will be subject to the APPs.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Whilst the APPs do not (in theory) apply differently to different cookies, the OAIC has issued public guidance about their distinctive operations and how individuals can adjust their browsing preferences accordingly.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

To date, the OAIC has not done so.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Not applicable.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The transfer of personal information to jurisdictions outside Australia is governed by APP 8. APP 8.1 requires that entities must take reasonable steps to ensure that a foreign recipient of personal information complies with the APPs. According to APP 8.2, however, this is not necessary where:

- it is reasonably believed that the recipient is subject to a law, or binding scheme, that bears overall substantial similarity to the APPs and the individual can take action to enforce such protections;
- the entity has obtained the individual's consent to the foreign disclosure;
- the foreign disclosure is required or authorised by Australian law;
- a permitted general situation (such as to lessen or prevent serious health and safety risks, or to take appropriate action in relation to suspected serious misconduct) applies;
- such disclosure is required by a government agency under an agreement to which Australia is a party; or
- the disclosure is by a government agency and relates to foreign law-enforcement activities.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

The OAIC espouses an expectation that, to take the necessary reasonable steps, entities transferring personal information to foreign recipients will enter into enforceable contracts requiring compliance with the APPs.

Under section 16C of the Privacy Act, if an entity has disclosed personal information on the basis of a belief that the foreign recipient will be APP-compliant (i.e. under APP 8.1), the Australian entity bears legal responsibility for any breaches of the APPs by the recipient.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

No. The entity itself must assess whether or not the foreign recipient will comply with the APPs or is subject to a similar privacy regime and, if necessary, seek the individual's consent only.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Protections of corporate whistle-blowers are provided for in the Corporations Act. This relates to the reporting of breaches of the Corporations Act or the *Australian Securities and Investments Commission Act 2001* (Cth). Whistle-blowers are protected from any litigation (civil or criminal), employment termination or victimisation as a result of their actions.

To qualify for these protections, a person must:

- be an officer, employee, or contractor of the company in question;
- make disclosure to a company auditor (or member of the audit team), officer or senior manager, person authorised to receive whistle-blower disclosure, or the Australian Securities and Investments Commission;
- give their name when making disclosure;
- have reasonable grounds to suspect a breach of relevant law may have occurred; and
- make the disclosure in good faith.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

To qualify as a whistle-blower under the Corporations Act, a person must provide their name when making disclosure.

On the other hand, whilst the Privacy Act is silent as to anonymous reporting, the OAIC requires the contact details of persons complaining to it about privacy breaches.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

In relation to federal government agencies, the *Surveillance Devices Act 2004* (Cth) provides broad authority for the use of 'optical surveillance devices' by law enforcement without a warrant. Whilst the use of CCTV specifically is regulated by the States, New South Wales, for example, mandates that CCTV be 'obvious and suitably visible', preferably with signage advising of its presence. On the other hand, Queensland requires that entities take 'reasonable steps' to make persons aware of their purpose and authority for using camera surveillance.

13.2 Are there limits on the purposes for which CCTV data may be used?

Again, this varies from state to state. However, as examples, both New South Wales and Queensland limit the collection of personal information by entities through CCTV to circumstances directly related to one of their functions.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

This varies by state. For example, New South Wales has dedicated legislation mandating consent or notice to legitimise the conduct of employee surveillance. On the other hand, Victorian law prohibits workplace surveillance in certain locations (e.g. bathrooms) but otherwise provides no additional restrictions over the general legal framework. The Queensland Law Reform Commission is currently examining workplace surveillance, with a review expected to be completed in 2020.

As best practice, the Australian Fair Work Ombudsman recommends that employers adhere to privacy standards consistent with the APPs. It is also advised that employers clearly advise employees of policies in relation to internet, phone and email use, as well as monitoring.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

In New South Wales, employees must be given at least 14 days' notice, or notice prior to their commencing work. This must include various details about the nature and extent of the monitoring.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no requirement under Australian privacy law for employee representatives or trade unions to be notified or consulted regarding employee monitoring.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

APP 11 stipulates that entities must take reasonable steps to protect personal information:

- from misuse, interference, and loss; and
- from unauthorised access, modification or disclosure.

The OAIC has stated that any APP entity that holds personal information (even those that could be considered processors) is responsible for compliance with the APPs. In cases of cross-border disclosure, see the discussion in section 11 above.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. The Privacy Act requires entities to notify the OAIC whenever an 'eligible data breach' occurs. Eligible data breaches involve unauthorised access to, or disclosure of, personal information that is likely to result in serious harm which the entity has not been able to negate with remedial action.

If it is not clear whether such a breach has occurred, entities must investigate in order to form their own assessment. The entity must take all reasonable steps to complete this within 30 days of becoming aware of information giving rise to its suspicion of the breach.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. The notification requirements referred to above in relation to the OAIC also apply to individuals whose personal data has been the subject of any such breach.

15.4 What are the maximum penalties for data security breaches?

The penalties for breaches of the Privacy Act, imposable by the OAIC, include requiring apologies and proposals of remedial measure, as well as civil penalties ranging in value up to $2.1 million.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Where the OAIC receives a privacy complaint, its powers under the Privacy Act include:

- making preliminary enquiries of any person;
- attempting conciliation of the complaint;
- investigating the complaint or ceasing to do so;
- requiring the production of information or documents, or the attendance of a person at a compulsory conference;
- entering a premises to inspect documents;
- accepting an enforceable undertaking; and
- making a determination of the complaint and seeking to enforce this in court.

Where the OAIC initiates an investigation on its own accord or by referral from another source, its powers under the Privacy Act include:

- assessing an entity's privacy practices and providing it with non-binding recommendations;
- accepting an enforceable undertaking;
- providing directions to an entity following the making of a determination in respect of the investigated action;
- bringing proceedings to enforce an undertaking or determination;
- seeking a court injunction to prevent a breach of the Privacy Act occurring;
- applying to a court for the imposition of a civil penalty order; and
- reporting to the Minister about the investigation (in certain circumstances, this is mandatory).

Criminal sanctions, such as a fine or term of imprisonment up to 12 months, may result from a failure to appear before, give information to, or provide false or misleading information to the OAIC when required to do so under the Act.

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The OAIC has the power to make legally binding rules and approve legally binding guidelines in respect of privacy issues. Current such instruments concern issues such as use of Tax File Numbers, medical research and genetic information. These instruments do not require any type of authorisation by court order.

The above instruments cover discrete issues only and otherwise the OAIC's 'hard' powers relate to specific cases, through making determinations in respect of particular complaints and accepting enforceable undertakings.

16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

In respect of the abovementioned guidelines, the OAIC has approved those issued by the National Health and Medical Research Council. The rules, on the other hand, are issued by the OAIC.

Where a complaint is made in respect of an alleged privacy breach, if conciliation does not resolve the matter, the OAIC may determine whether a breach has occurred and, if so, what remedies should be ordered. In 2018, the OAIC found that a superannuation fund had unlawfully disclosed personal information of its members to third parties. As a result, an apology was ordered.

In other cases where an entity has cooperated with an investigation/enquiry by the OAIC, or in response to a privacy complaint, the OAIC may accept an enforceable undertaking to ensure future compliance with privacy law. In late 2018, the OAIC accepted an undertaking from the Department of Health following the release of data concerning patients' claims for public medical benefits.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Whilst the predominant focus of the OAIC is directed towards businesses and companies established domestically, the OAIC does take action in respect of foreign organisations. For example, in 2016 the OAIC, having worked with the Privacy Commissioner of Canada, obtained an enforceable undertaking from a Canadian-based media company in respect of concerns over security of personal information, retention and accuracy of data, as well as compliance reporting, monitoring and enforcement.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Although APP 8.2 allows the disclosure of information to an overseas recipient where required/authorised by law, this is restricted to Australian legislation and courts/tribunals. It does not apply to requests from foreign law enforcement agencies, which remain subject to APP 8.1 (requiring the taking of reasonable steps to ensure that the overseas recipient does not breach the APPs).

Under section 6A(4) of the Privacy Act, a business acting outside Australia, and as required by an applicable foreign law, will not breach the APPs. This is notwithstanding the extraterritorial reach of the Privacy Act, detailed above.

Australia is also party to a number of international treaties and conventions that relate to the sharing of data across national borders. Although concerning the actions of public bodies, not businesses, they are of central relevance to the sharing of Australian information with foreign law enforcement. These instruments include the following examples:

A. The 'Five Eyes' is an intelligence pact between Australia, the United States, the United Kingdom, New Zealand and Canada, all parties to the *UKUSA Agreement*. Part of this arrangement is 'critical information sharing' between the nations that relates to issues of law enforcement, border protection and criminal justice. These partners also share information concerning financial sector intelligence.

B. Australia is party to over 25 bilateral mutual legal assistance treaties with foreign nations. All these treaties contain provisions explicitly contemplating the exchange of information between governments in relation to criminal matters.

C. Australia is a party to the multilateral 2001 *Budapest Convention on Cybercrime*. Over 70 nations are parties to this treaty. The Budapest Convention covers a range of issues related to international cyber-crime, including requests to/from foreign states for the seizure, collection and interception of computer data. Article 26 specifically contemplates the spontaneous sharing of information between nations, without any prior request, that may be used in the investigation or prosecution of cyber-crime offences.

D. Australia is also party to a number of Taxation Information Exchange Agreements ('**TIEAs**') with states outside the Organisation for Economic Cooperation and Development. TIEAs facilitate the exchange of information between countries concerning taxation matters and are aimed at combatting international tax avoidance.

17.2 What guidance has/have the data protection authority(ies) issued?

The OAIC has issued guidance to businesses on this issue as part of its commentary to APP 8. The OAIC recommends that APP entities notify the individual that it may be required to disclose personal information under a foreign law, and that this would not breach the APPs. It is also suggested that any entity involved in regular foreign disclosure of personal information should include this in its notice under APP 5.

In relation to information shared through international treaties and conventions, such as those described above, Australia is party to numerous international agreements governing the protection of information shared across borders. These agreements cover issues such as security classification, protective measures, and procedures for the exchange of such information.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

A major recent development in Australian privacy law was the passing of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth) ('Assistance and Access Act') on the final sitting day of Federal Parliament for 2018, following a period of public consultation. The Assistance and Access Act contains an array of legislative reforms granting government agencies greater powers to access computer data and communications.

A prominent aspect of the Act is the power of government agencies to issue compulsory Technical Assistance Notices ('**TAN**') and Technical Capability Notices ('**TCN**') to communications providers, essentially requiring private organisations to aid public law enforcement actions. The issuing of a TAN will require a provider to assist an agency through action such as removing electronic protections (e.g. decrypting communications), providing technical information, utilising software nominated by the agency, or facilitating access to devices/service, etc. On the other hand, a TCN requires a communications provider to develop a new capability to

assist the government agency, and can cover anything that could be the subject of a TAN, except the removal of electronic protections.

The scope of legislation affected by the Assistance and Access Act is broad, stretching from the Crimes Act 1914 to the Mutual Assistance in Criminal Matters Act 1987, to the Telecommunication Act 1997. Although passed into law, the Parliamentary Joint Committee on Intelligence and Security is due to further report on this Act in April 2019.

18.2 What "hot topics" are currently a focus for the data protection regulator?

Health records, in particular the introduction of the 'My Health Record' system – containing online summaries of personal health information – have been the subject of much recent attention, including the extension into 2019 of a public opt-out period. The OAIC has issued a wide array of public guidance on privacy issues that may be associated with this system.

The early operation of the Notifiable Data Breaches scheme continues to receive attention from the OAIC, including through the publication of a guide for entities dealing with such data breaches.

Acknowledgment

The authors would like to thank Liam MacAndrews, Solicitor, for his invaluable contribution to the writing of this chapter. Liam assists the Partners on international criminal law cases and cross-border investigations.

Dennis Miralis

Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: dm@ngm.com.au
URL: www.ngm.com.au

Dennis Miralis is a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-jurisdictional regulatory investigations and prosecutions. His areas of expertise include bribery and corruption, global tax investigations, proceeds of crime, anti-money laundering, worldwide freezing orders, cybercrime, national security law, Interpol Red Notices, extradition and mutual legal assistance law. Dennis advises individuals and companies under investigation for economic crimes both locally and internationally. He has extensive experience in dealing with all major Australian and international investigative agencies.

Phillip Gibson

Nyman Gibson Miralis
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: pg@ngm.com.au
URL: www.ngm.com.au

Phillip Gibson is one of Australia's leading criminal defence lawyers, with over 30 years of experience in all areas of criminal law. Phillip has significant experience in transnational cases across multiple jurisdictions often involving: white-collar and corporate crime; assets forfeiture; money laundering and proceeds of crime; extradition; mutual assistance; Royal Commissions; bribery and corruption; and ICAC and Crime Commissions matters. He has extensive experience in dealing with all major Australian and international investigative agencies.

NYMAN GIBSON MIRALIS
Criminal Defence Lawyers and Advisors est. 1966

Nyman Gibson Miralis is an international award-winning criminal defence law firm based in Sydney, Australia. For over 50 years it has been leading the market in all aspects of general, complex and international crime, and is widely recognised for its involvement in some of Australia's most significant criminal cases.

Our international law practice focuses on white-collar and corporate crime, transnational financial crime, bribery and corruption, international money laundering, cybercrime, international asset freezing or forfeiture, extradition and mutual assistance law.

Nyman Gibson Miralis strategically advises and appears in matters where transnational cross-border investigations and prosecutions are being conducted in parallel jurisdictions, involving some of the largest law enforcement agencies and financial regulators worldwide.

Working with international partners, we have advised and acted in investigations involving the USA, Canada, the UK, the EU, China, Hong Kong, Singapore, Taiwan, Macao, Vietnam, Cambodia, Russia, Mexico, South Korea, British Virgin Islands, New Zealand and South Africa.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com