ICLG

The International Comparative Legal Guide to:

Data Protection 2017

4th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bae, Kim & Lee LLC
Bagus Enrico & Partners
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Cuatrecasas
Dittmar & Indrenius
Drew & Napier LLC
Ecija Abogados
ErsoyBilgehan
Eversheds Sutherland
GANADO Advocates
Gilbert + Tobin
GRATA International
Hacohen & Co.
Herbst Kinsky Rechtsanwälte GmbH
Hunton & Williams
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys-at-Law
LPS L@w
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at Law Ltd.
Portolano Cavallo
Rato, Ling, Lei & Cortés Lawyers
Rossi Asociados
Subramaniam & Associates (SNA)
Wikborg Rein Advokatfirma AS

global legal group

global legal group

Contributing Editors
Anita Bapat and Aaron P. Simpson, Hunton & Williams

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Paul Mochalski

Sub Editor
Hollie Parker

Senior Editors
Suzie Levy, Rachel Williams

Chief Operating Officer
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
May 2017

ISBN 978-1-911367-50-5
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

Chapter 2

Australia


Melissa Fai


Alex Borowsky

Gilbert + Tobin

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

In Australia, the collection, use, storage and disclosure of 'personal information' is principally regulated by the federal *Privacy Act 1988* (**Privacy Act**).

The Privacy Act applies to the handling of personal information by, amongst others, Australian federal government agencies and private sector organisations. Pursuant to a 'small business exception' and with important qualifications (including when providing services pursuant to government contracts) and jurisdictional nexus requirements, generally private sector organisations are only regulated when their annual revenue (including revenue of related entities) is greater than AU$3 million.

Some small business operators (organisations with a global aggregate group turnover of AU$3 million or less) are also covered by the Privacy Act including:

- private sector health services providers;
- businesses that sell or purchase personal information;
- credit reporting bodies; and
- contracted service providers for a Commonwealth (federal government agency) contract.

The Privacy Act includes:

- Thirteen Australian Privacy Principles (**APPs**) which apply to the handling of personal information by government agencies and private sector organisations collectively referred to as 'APP entities'; and
- credit reporting provisions which apply to the handling of personal credit information about individuals by credit reporting bodies, credit providers and some other third parties.

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

There are a range of laws in Australia, both at the federal and state and territory level, which impact data protection.

These include:

- state and territory privacy legislation, applying to personal information held by government agencies and private sector contractors to government agencies (for example, the *Privacy and Personal Information Protection Act 1988* (NSW)). State and Territory Privacy, Information or Health Information Commissioners administer such legislation;
- federal law requiring telecommunications carriers and carriage service providers to capture and retain certain information about communications carried over services provided by them;
- federal and state and territory laws governing telecommunications interception and access to stored communications, the use of surveillance devices, tracking devices and listening devices, video and audio-visual monitoring of public places and workplaces and computer and data surveillance of workplaces (including home working);
- federal and state/territory freedom of information legislation, applying to information held by government agencies;
- *Data-matching Program (Assistance and Tax) Act 1990* (Cth) which regulates the federal government data-matching using tax file numbers (TFN). *The Privacy (Tax File Number) Rule 2015* issued under the Privacy Act also regulates the collection, storage, use, disclosure, security and disposal of individuals' TFN by public agencies and private organisations;
- *Spam Act 2003* (Cth) (**Spam Act**), which deals with the sending of unsolicited commercial electronic messages, including emails and SMS;
- *Do Not Call Register Act 2006* (Cth) (**DNCR Act**), regulating unsolicited commercial calling to telephone numbers listed on the national Do Not Call Register (**DNCR**);
- federal and state criminal laws dealing with unauthorised access to computer systems, including databases;
- federal and state law criminalising publication of so-called 'revenge porn' (as at the date of writing the *Criminal Code Amendment (Private Sexual Material) Bill 2015* was before the Australian Parliament); and
- developing judge-made law in the form of an equitable doctrine of misuse of confidential information.

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

The Australian health sector is subject to additional and specific statutory restrictions in relation to data protection due to the sensitive nature of health information under:

- *My Health Records Act 2012*, *My Health Records Rule 2016* and *My Health Records Regulation 2012*, which creates the legislative framework for the Australian Government's My Health Record system. The My Health Records Act limits when and how health information included in a My Health Record can be collected, used and disclosed. Unauthorised collection, use or disclosure of My Health Record information is both a breach of the My Health Records Act and an interference with privacy. The Office of

the Australian Information Commissioner (**OAIC**) regulates the handling of personal information under the My Health Record system by individuals, Australian Government agencies, private sector organisations and some state and territory agencies (in particular circumstances);

- *Healthcare Identifiers Act 2010* (Cth), regulating (among other things) the use and disclosure of healthcare identifiers; and
- state and territory health information protection acts. For example, the *Health Records Act 2001* (Vic) and the *Health Records and Information Privacy Act 2002* (NSW) govern the handling of health information in both the public and private sectors in Victoria and NSW respectively.

The telecommunications sector is also subject to additional and specific statutory restrictions under:

- Part 13 of the *Telecommunications Act 1997* (Cth), which imposes restrictions on the use and disclosure of telecommunications and communications-related data;
- the *Telecommunications (Interception and Access) Act 1979* (Cth), which, among other things, regulates the interception of, and access to, the content of communications transiting telecommunications networks and stored communications (e.g. SMS and emails) on carrier networks with enforcement agencies. This Act also includes the new data retention scheme which requires telecommunications carriers and internet service providers to retain certain telecommunications data; and
- mandatory industry codes of practice administered by the Australian Communications and Media Authority and governing (among other things) telecommunications data relating to consumers.

1.4 What is the relevant data protection regulatory authority(ies)?

The Privacy Act is administered by the Australian Privacy Commissioner (the **Commissioner**) which is integrated within the OAIC.

The OAIC is responsible for enforcing compliance with the Privacy Act and reviewing proposed privacy codes.

The Australian Communications and Media Authority (**ACMA**) enforces provisions of the Spam Act and the DNCR Act. It also administers a number of privacy affecting codes in the communications sector.

The Australian Attorney-General's Department administers provision of lawful assistance to law enforcement agencies under the *Telecommunications (Interception and Access) Act 1979* (Cth), an active role in regulating and enforcing privacy-related legislative schemes.

State and territory Privacy, Information or Health Information Commissioners administer state and territory privacy legislation, applying to personal information held by respective state and territory government agencies and private sector contractors to government agencies, and in some states and territories, health service providers in the commercial health sector as well as public sector health service providers. In some states and territories, these Commissioners also oversee the state and territory laws affecting use of surveillance devices, tracking devices and listening devices, video and audio-visual monitoring of public places and workplaces and computer and data surveillance of workplaces (including home working).

2 Definitions

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

- "**Personal Data**"

  'Personal information' under the Privacy Act means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material from or not.

  Whether an individual is 'reasonably identifiable' from particular information will depend on considerations that include:

  - the nature and amount of information;
  - the circumstances of its receipt;
  - who will have access to the information;
  - other information either held by or available to the APP entity that holds the information;
  - whether it is possible for the individual or entity that holds the information to identify the individual, using available resources (including other information available to that individual or entity). Where it may be possible to identify an individual using available resources, the practicability, including the time and cost involved, will be relevant to deciding whether an individual is 'reasonably identifiable'; and
  - if the information is publicly released, whether a reasonable member of the public who accesses that information would be able to identify the individual.

- "**Sensitive Personal Data**"

  'Sensitive information' means information or an opinion about an individual's:

  - racial or ethnic origin;
  - political opinions;
  - membership of a political association;
  - religious beliefs or affiliations;
  - philosophical beliefs;
  - membership of a professional or trade association;
  - membership of a trade union;
  - sexual orientation or practices; or
  - criminal record,

  that is also personal information; or

  - health information about an individual;
  - genetic information about an individual that is not otherwise health information;
  - biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
  - biometric templates.

- "**Processing**"

  The term 'processing' is not used in the Privacy Act. Processing would constitute a 'use' of personal information under the Privacy Act. 'Use' and 'disclosure' are key concepts. Under the Privacy Act, the Commissioner may issue guidelines regarding acts or practices that may have an impact on the privacy of individuals. The APP guidelines include the following guidance about these terms:

  - 'Use' – generally, an APP entity uses personal information when it handles and manages information within the entity's effective control.

- 'Disclosure' – an APP entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.

- "**Data Controller**"

  The term 'data controller' is not used in the Privacy Act and state and territory privacy acts.

  Subject to jurisdictional nexus and the 'small business exception', organisations and government agencies that collect, use or disclose personal information are regulated in relation to those activities. Organisations and federal government agencies that collect, use or disclose personal information are called 'APP entities' and must comply with the Privacy Act and the APPs contained in the Privacy Act.

  In practice, an important and difficult distinction is between APP entities that collect, use or disclose personal information and organisations that as sub-contractors to those APP entities may handle personal information for those entities: for example, operations of data warehouses or data centres and cloud as-a-service providers.

  Where personal information is entrusted by an APP entity that collects that personal information to another party for storage and processing, the Commissioner looks to whether the second party has 'control' of that information. If the second party can fully access and edit that information, the provision of that personal information to the second party is a 'disclosure' subject to relevant notice and consent requirements and the second party is an entity that 'collects' this information. However, the Commissioner has expressed the view that in limited circumstances, an APP entity might retain such a degree of control over the information that the APP entity is considered to be 'using' that information and not disclosing the information to the second party. For example, where an APP entity provides personal information to a cloud service provider located overseas, this may be a 'use' if the information is provided for the limited purpose of performing the services of storing and ensuring the APP entity may access the personal information, and a binding contract between the parties:

  - requires the provider only to handle the personal information for these limited purposes;
  - requires any subcontractors to agree to the same obligations; and
  - gives the entity effective control of how the personal information is handled by the provider. Issues to consider include whether the entity retains the right or power to access, change or retrieve the personal information, who else will be able to access the personal information and for what purposes, what type of security measures will be used for the storage and management of the personal information and whether the personal information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.

  Whether or not other examples are considered a 'use' or a 'disclosure' will depend on the circumstances of each individual case, having regard to the degree of control held by the APP entity.

- "**Data Processor**"

  The term 'data processor' is not used in the federal Privacy Act and state and territory privacy acts. See the discussion as to 'Data Controller' in the last paragraph.

- "**Data Subject**"

  Where personal information about any individual is handled (collected, used or disclosed) by a relevant entity, being (in the case of the Privacy Act, subject to jurisdictional nexus and the 'small business exception') any APP entity, that individual is protected by the APPs.

  It is not relevant whether that individual resides in Australia or is physically present in Australia or provided the personal information directly to the APP entity.

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

  "**Australian Link**"

  The APPs have extra-territorial application and will extend to an act done, or practice engaged in, outside Australia by an organisation, or small business operator, that has an 'Australian link' (s 5B(1A)).

  An organisation or small business operator has an Australian link if the organisation or operator is:

  - an Australian citizen or a person whose continued presence in Australia is not subject to a legal time limitation;
  - a partnership formed, or a trust created, in Australia or an external territory;
  - a body corporate incorporated in Australia or an external territory; or
  - an unincorporated association that has its central management and control in Australia or an external territory.

  An organisation that does not fall within one of those categories will also have an Australian link where both of the following apply:

  - it carries on business in Australia or an external territory; and
  - it collected or held personal information in Australia or an external territory, either before or at the time of the act or practice.

  "**Collects**"

  An APP entity collects personal information only if the entity collects the personal information for inclusion in a record or generally available publication.

  "**De-identified**"

  Personal information is 'de-identified' if the information is no longer about an identifiable individual or an individual who is reasonably identifiable. The Commissioner notes that de-identification includes two steps: removing personal identifiers, such as an individual's name, address, date of birth or other identifying information; and removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.

  De-identification can be effective in preventing re-identification of an individual, but may not remove that risk altogether. There may, for example, be a possibility that another dataset or other information could be matched with the de-identified information. The risk of re-identification must be actively assessed and managed to mitigate this risk. This should occur both before an information asset is de-identified and after disclosure of a de-identified asset.

  "**Holds**"

  A number of APPs (such as APPs 6, 11, 12 and 13) apply to an APP entity that 'holds' personal information.

  An entity 'holds' personal information 'if the entity has possession or control of a record that contains the personal information'. The term 'holds' extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with. This means that one entity can physically possess personal information that another entity controls. In such situations, both entities will 'hold' the information at the same time. If each entity is covered by the Privacy Act, each will have separate responsibilities in relation to handling that information under the Privacy Act.

3 Key Principles

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

- **Transparency**

  The object of APP 1 is to ensure that APP entities manage personal information in an open and transparent way. This includes the obligation that an APP entity has a clearly expressed and up-to-date privacy policy available to the public free of charge and in an appropriate form. Practices and processes must also reflect the stated privacy policy: the Commissioner has interpreted APP 1 as requiring implementation of 'privacy by design' into an APP entity's business practices.

  APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps, at or before the time of collection, or as soon as practicable afterwards, either to notify the individual of certain matters or to ensure the individual is aware of those matters. APP 5.2 lists the matters that must be notified to an individual or of which they must be made aware.

  The requirement to notify or ensure awareness of the APP 5 matters applies to all personal information 'collected' about an individual, either directly from the individual or from a third party.

- **Lawful basis for processing**

  The global Privacy Act governs the collection, holding, use, disclosure, access and correction of personal information by APP entities. It does not refer to the concept of "processing" and governs each of these activities wherever the relevant act or practice is carried out by or for an APP entity. The Act prohibits an organisation from collecting personal information unless the information is reasonably necessary for, or directly related to, one or more of the organisation's functions or activities.

  The state and territory privacy legislation apply analogous concepts in relation to entities regulated by those Acts.

- **Purpose limitation**

  In accordance with APP 6, an APP entity can only use or disclose personal information for the particular purpose for which it was collected (known as the 'primary purpose'), or for a 'secondary purpose' if an exception applies.

  Use or disclosure of personal information for a 'secondary purpose' is permitted under specific exceptions where that secondary use or disclosure is:

  - consented to by the individual;
  - one to which the individual would reasonably expect the APP 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;
  - required or authorised by or under an Australian law or a court/tribunal order;
  - necessary to lessen or prevent a serious threat to any individual's life, health or safety, or to public health or safety, and it is unreasonable or impracticable to obtain the consent of the individual;
  - necessary in order for an organisation to take appropriate action in relation to a reasonable suspicion of unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities. APP 6.2(e) also permits the use or disclosure of personal information for a secondary purpose to an enforcement body for one or more enforcement related activities;
  - in the conduct of surveillance activities, intelligence gathering activities or monitoring activities, by a law enforcement agency;
  - the conduct of protective (for example, in relation to children) or custodial activities;
  - to assist any APP entity, body or person to locate a person who has been reported as missing (where the entity reasonably believes that this use or disclosure is reasonably necessary, and where that use or disclosure complies with rules made by the Commissioner);
  - for the establishment, exercise or defence of a legal or equitable claim; or
  - for the purposes of a confidential alternative dispute resolution process.

  Section 13B(1)(b) provides that where a body corporate discloses personal information (other than sensitive information) to a related body corporate, this is generally not considered 'an interference with the privacy of an individual' under the Privacy Act. This provision applies to related bodies corporate and not to other corporate relationships, such as a franchise or joint-venture relationship. The effect of this provision is that an APP entity may disclose personal information (other than sensitive information) to a related body corporate without relying on other exceptions under the Act and in particular APP 6.2.

- **Data minimisation**

  Under APP 3, an organisation must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

- **Proportionality**

  Under APP 10, APP entities are required to ensure that the personal information they use or disclose is accurate, up-to-date, complete and relevant.

- **Retention**

  In accordance with APP 11.2, where an APP entity holds personal information about an individual which is no longer needed for any purpose for which the information may be used or disclosed, the APP entity must take such steps as are reasonable in the circumstances to destroy or de-identify the information.

  APPs 4.3 and 11.2 require the destruction or de-identification of personal information in certain circumstances. Where the information is contained in a Commonwealth (federal) record (which is the property of the Commonwealth), or is required to be retained under Australian law or by a court or tribunal, the information must be retained. For example, financial records must be retained under the *Corporations Act 2001* (Cth) for seven years.

- *Other key principles – please specify*

  - **Collection by lawful and fair means**

    An APP entity must collect personal information 'only by lawful and fair means' (APP 3.5). This requirement applies to all APP entities. Examples of where a collection of personal information may be unfair (some may also be unlawful) include collecting from an electronic device which is lost or left unattended, collecting from an individual who is traumatised, in a state of shock or intoxicated, collecting in a way that disrespects cultural differences or after misrepresenting the purpose or effect of collection, or the consequences for the individual of not providing the requested information.

  - **Collecting directly from the individual**

    APP 3.6 provides that an APP entity 'must collect personal information about an individual only from the individual', unless one of the following exceptions applies:

- for all APP entities, it is unreasonable or impracticable for the entity to collect personal information only from the individual;
- for government agencies, the individual consents to the personal information being collected from someone other than the individual; and
- for government agencies, the agency is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual.

- **Direct marketing**

  APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies.

  Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services. Examples include displaying an advertisement on a social media site that an individual is logged into, using personal information, including personal data collected by cookies relating to websites the individual has viewed, or sending an email to an individual about a store sale, or other advertising material relating to the store, using personal information provided by the customer in the course of signing up for a store loyalty card.

  Where an organisation is permitted to use or disclose personal information for the purpose of direct marketing, it must always: allow an individual to request not to receive direct marketing communications (also known as 'opting out'); and comply with that request.

- **Cross-border disclosure of personal information**

  Before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information (APP 8.1).

  An APP 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 APPs (s 16C).

  There are exceptions to the requirement in APP 8.1 to take reasonable steps and to the accountability provision in s 16C.

- **Security of personal information**

  APP 11 requires an APP entity to take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information. An APP entity that holds personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure (APP 11.1). Unauthorised access includes both access by an employee of the entity or independent contractor and unauthorised access by an external third party (such as by hacking).

  Reasonable steps should include, where relevant, taking steps and implementing strategies in relation to governance, culture and training, internal practices, procedures and systems, ICT security, access security, third party providers (including cloud computing), data breaches, physical security, destruction and de-identification and compliance with applicable standards.

  The Commissioner not infrequently determines that internal or external data breaches are reasonably attributable to a failure by an APP entity to take reasonable steps to protect information security or to take reasonable steps to destroy personal information or ensure it is de-identified if it no longer needs the information for any purpose for which it may be used or disclosed under the APPs.

4 Individual Rights

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

- **Access to data**

  An APP entity that holds personal information about an individual must, on request, give that individual access to the information (APP 12.1).

  APP 12 also sets out minimum access requirements, including the time period for responding to an access request, how access is to be given, and that a written notice, including the reasons for the refusal, must be given to the individual if access is refused. For example, an APP entity must respond to a request for access to the personal information if the entity is an agency, within 30 days after the request is made, or if the entity is an organisation, within a reasonable period after the request is made.

  There are a number of exceptions to the obligation for organisations to provide an individual access to their personal information, including where the entity reasonably believes that:

  - giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
  - giving access would have an unreasonable impact on the privacy of other individuals.

- **Correction and deletion**

  APP 13.1 provides that an APP entity must take reasonable steps to correct personal information it holds, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held.

  APP 13.1 requires an APP entity to take reasonable steps to correct personal information it holds, in two circumstances: on its own initiative; and at the request of the individual to whom the personal information relates.

  Upon receiving a request, an entity must decide if it is satisfied that the information is incorrect, and if so, take reasonable steps to correct it.

  APP 13 does not stipulate formal requirements that an individual must follow to make a request, require that a request be made in writing, or require the individual to state that the request is an APP 13 request.

- **Objection to processing**

  There is no general right for an individual to object to collection, use, or disclosure of personal information. The Privacy Act generally requires notice to individuals as to these activities and consent in relation to particular activities, notably including collection, use or disclosure of sensitive information and use and disclosure of personal information for the purpose of direct marketing.

  APP 2 provides that individuals must have the option of dealing anonymously or by pseudonym with an APP entity. However, an APP entity is not required to provide those options where:

  - the entity is required or authorised by law or a court or tribunal order to deal with identified individuals; or
  - it is impracticable for the entity to deal with individuals who have not identified themselves.

  Anonymity means that an individual dealing with an APP entity cannot be identified and the entity does not collect personal information or identifiers.

  A pseudonym is a name, term or descriptor that is different to an individual's actual name.

Where applicable, an APP entity must ensure that individuals are made aware of their opportunity to deal anonymously or by pseudonym with the entity.

- **Objection to direct marketing**

  If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

  There are exceptions to this prohibition. Generally, organisations may use or disclose personal information for direct marketing purposes where the individual has either consented to their personal information being used for direct marketing, or the individual has a reasonable expectation that their personal information will be used for this purpose, and the organisation meets a number of conditions relating to provision of a convenient opt-out mechanism.

  The Spam Act and the DNCR Act contain specific provisions regarding particular forms of direct marketing.

  The Spam Act regulates the sending of commercial electronic messages, which relevantly includes unsolicited emails, SMS and MMS where promotion of goods or services is one purpose of the message. It is unclear whether unsolicited promotional postings to social media pages may be 'messages' that are regulated as 'spam'.

  The DNCR Act regulates telemarketing voice calls, limiting the hours in which such calls may be made and prohibiting telemarketing to telephone numbers that account holders have elected to list on the DNCR.

  Although the drafting of APP 7.8 is not clear, it appears to be the legislature's intention that where those Acts impose particular prohibitions, restrictions or requirements, these will apply and, to the extent of any inconsistency, APP 7 will not apply. It also appears to be the legislature's intention that APP 7 may also operate in relation to unsolicited commercial electronic messages and telemarketing to the extent that APP 7 is not inconsistent with other relevant Acts. It follows that each of the Acts referred to above must be considered and applied in relation to any prospective direct marketing activity involving commercial electronic messaging or outbound voice telemarketing.

- **Complaint to relevant data protection authority(ies)**

  An individual has the right to lodge a complaint with the Commissioner for alleged breaches of the Privacy Act. Generally, the complainant must first register a complaint with the APP entity to which the complaint relates. If dissatisfied with the response, a complainant can complain to the Commissioner or to an external dispute resolution scheme of which the entity is a member (if applicable). In conducting its investigations, the Commissioner may require the production of documents and information, and compel people to appear and answer questions.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

There are no registration or notification requirements under the Privacy Act or state or territory privacy acts.

5.2 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.

5.3 Who must register with/notify the relevant data protection authority(ies)? (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.

5.4 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.

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

This is not applicable.

5.6 What is the fee per registration (if applicable)?

This is not applicable.

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

This is not applicable.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

This is not applicable.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

This is not applicable.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

Optional. The Privacy Act and state or territory privacy acts do not expressly require an APP entity to appoint a data protection officer.

However, APP 1 requires an entity to implement practices, procedures and systems that will ensure its compliance with the Privacy Act and enable it to deal with inquiries or complaints. The appointment of a data protection or privacy officer may be one of

the many steps an entity can take to meet this obligation. An APP Privacy Policy must explain the procedure an individual can follow to gain access to or seek correction of personal information the APP entity holds (APP 1.4(d)). At a minimum, the policy should state:

- that individuals have a right to request access to their personal information and to request its correction (APPs 12 and 13); and
- the position title, telephone number, postal address and email address of a contact person for requests to access and correct personal information. An APP entity could establish a generic telephone number and email address that will not change with staff movements (for example, privacy@agency.gov.au).

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

This is not applicable in Australia.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

As noted in the response to question 6.1, the appointment of a data protection or privacy officer may assist an APP entity to meet its obligation to implement practices, procedures and systems that will enable it to deal with inquiries or complaints about its compliance with the Privacy Act. The Commissioner recommends consideration of governance mechanisms to ensure compliance with the APPs, such as designated privacy officers and regular reporting to the entity's governance body.

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

There are no specific requirements.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

Data protection or privacy officers are typically responsible for overseeing implementation of an APP entity's privacy compliance strategy, including verifying that processes and practices conform with stated policy and statutory requirements. Activities may include designing and facilitating staff privacy training, data flow mapping, either commissioning or undertaking privacy impact assessments, consulting with information security teams as to steps to protect information security, developing both external and internal-facing privacy policies and dealing with complaints regarding the entity's handling of personal information.

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

No, they do not.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

Electronic marketing is partly regulated through subject matter-specific federal laws such as the Spam Act, which governs most forms of electronic marketing, and the DNCR Act, which regulates unsolicited telemarketing calls.

APP 7 of the Privacy Act also regulates use or disclosure of personal information for the purpose of direct marketing activities: see further section 4 (objection to direct marketing) above.

Generally, organisations may only use or disclose personal information for direct marketing purposes where the individual has either consented (expressly or impliedly) to their personal information being used for direct marketing, or has a reasonable expectation that their personal information will be used for this purpose, and conditions relating to provision by the organisation of an opt-out mechanism are met.

The Spam Act prohibits 'unsolicited commercial electronic messages' with an 'Australian link' from being sent or caused to be sent. Commercial electronic messages may only be sent with an individual's consent (express or inferred in certain circumstances), and the message contains accurate sender identification and a functional unsubscribe facility. The burden of proving consent lies with the sender of the message.

Voice calls, including synthetic or recorded calls (such as robocalls), are separately regulated under a 'do not call' regulatory framework established under the DNCR Act and associated legislation and instruments, including the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**), under which individuals may complain about potential breaches of the Spam Act and the DNCR Act, and the *Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Industry Standard 2007* (**DNCR Industry Standard**). Marketing faxes are also regulated. A telemarketing call or marketing fax is broadly defined as a voice call or fax made to a number to offer, supply, provide, advertise or solicit goods or services, land or an interest in land, a business/investment opportunity and donations. Certain calls are not considered to be telemarketing or fax marketing, including product recall, fault verification, appointment rescheduling, appointment reminder, payments and solicited calls/faxes about orders, requests or customer enquiries.

The DNCR Act provides an 'opt-out' option, allowing Australians who do not wish to receive telemarketing calls or marketing faxes to list their private-use fixed and mobile telephone numbers and fax numbers on the DNCR. As at March 2017, total DNCR registrations exceed 10.35 million. The quantity of numbers that telemarketers and fax marketers submit for checking (or 'washing') against the DNCR rise month by month: as at March 2017, 90 million numbers are checked against the DNCR per month.

Unsolicited telemarketing calls or faxes must not be made to an Australian number registered on the DNCR without the consent (implied or express) of the relevant account holder or their nominee.

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

The ACMA is very active in enforcing the provisions of the Spam Act and the DNCR. In most cases, the ACMA will, as an initial step, issue a formal warning to entities that breach the Acts. However, the ACMA also regularly accepts enforceable undertakings and issues infringement notices to address non-compliance with the Spam Act and the Do Not Call Register Act.

The ACMA publishes its ACMA compliance and enforcement policy, available at www.acma.gov.au. The graduated model used by the ACMA to respond to potential non-compliance ranges from encouraging voluntary compliance and informal resolution to administrative action and, where necessary, civil action.

Between 2015 and 2016, the ACMA finalised eight DNCR Act and five Spam Act-related investigations under Part 26 of the Telecommunications Act and took seven enforcement actions, three formal warnings, three infringement notices and one Federal Court proceeding. (In March 2016, the ACMA commenced Federal Court proceedings against a travel agent company and its director. In June 2016, the Court ordered the company to pay AU$150,000 for breaching the DNCR Act and AU$150,000 for breaching the DNCR Industry Standard. The director was ordered to pay penalties totalling AU$25,000 for being knowingly concerned in, or a party to, the company's breaches.) In previous years, the ACMA issued a AU$20,400 infringement notice to a company that made telemarketing calls to telephone numbers listed on the DNCR and a AU$15,500 infringement notice to a company that sent spam emails that did not include adequate contact information or a functional unsubscribe facility. Since 2003, the ACMA has completed five prosecutions in the Federal Court involving 14 respondents and resulting in AU$30.4 million in penalties. In another case involving the DNCR Act, the ACMA also obtained a five-year injunction that restricted the respondent from engaging in the telemarketing sector.

The OAIC also actively investigates and enforces alleged breaches of the Privacy Act in relation to the use and disclosure of personal information for direct marketing activities. In most cases, the OAIC will seek to conciliate any complaints as to alleged breaches of the direct marketing restrictions in APP 7.

The OAIC publishes its privacy regulatory action policy and a guide to privacy regulatory action, available at www.oaic.gov.au/about-us/our-regulatory-approach.

7.3 Are companies required to screen against any "do not contact" list or registry?

No, but prohibition on making unsolicited calls or faxes to a number on the DNCR does not apply if:

- the telemarketer or fax marketer had washed their list in the last 30 days and the number was not on the register;
- the relevant phone or fax account-holder or their nominee consented to the call or fax; and
- the call or fax was made or sent (or caused to be made or sent) by mistake and the person took reasonable precautions, and exercised due diligence, to avoid the contravention.

Express consent may occur where individuals, or their nominees, have specifically agreed to receive telemarketing calls or marketing faxes. Importantly, where express consent has not been given for a set period or indefinitely, consent is taken to expire three months after it was given.

In the absence of expressed consent to receive telemarketing calls or marketing faxes, consent may still be able to be reasonably inferred from both an individual's conduct and business or other relationships. For example, it is reasonable that a person who holds an XYZ Bank credit card may expect to receive calls about XYZ Bank home loans or XYZ Bank savings products. If consumers indicate they do not wish to receive telemarketing calls or marketing faxes from an organisation, consent ends immediately and can no longer be inferred.

Washing against the list on a monthly basis provides the most readily verifiable basis for compliance.

There is no 'do not spam' equivalent or email, SMS and MMS, partly because each unsolicited electronic communication is spam unless there was prior consent of the recipient: that is, the onus is upon the sender to establish express or inferred consent of the receipt of the first and each subsequent email, SMS or MMS.

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

The ACMA may prosecute a person in the Federal Court and seek fines. The penalty units referred to in the Spam Act are equal to AU$180 each. For example, the penalty under section 25(5)(b) of the Spam Act for a company with a previous record of spamming and who sent two or more spam messages on a given day without consent is a maximum fine of 10,000 penalty units, equating to a maximum penalty of AU$1,800,000 (for each day).

The Commissioner may determine a range of remedies for breaches of the direct marketing provisions in APP 7, including a declaration that compensation should be paid for any loss or damage suffered by the complainant. In addition, serious or repeated breaches of the APPs, including APP 7, are punishable by civil penalties of up to AU$1.8 million.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

The Privacy Act contains no cookie or technology-specific rules. To the extent that the use of cookies involves the collection, use or disclosure or transfer of personal information, the APPs will apply. The concept of 'collection' of personal information applies broadly, and includes information associated with web browsing, such as personal information collected by cookies. Collection of personal information using cookies could occur provided that the notice and consent requirements were followed, although any responsive electronic communication would likely be regulated as requiring prior consent either as direct marketing under APP 7 or spam under the Spam Act (depending upon the nature of that responsive communication).

Analytical information collected from cookies (e.g., the number of times a page was visited) will not be personal information under the Privacy Act unless an individual is reasonably identifiable. See further *OAIC, Privacy Fact Sheet 4 – Online behavioural advertising: Know your choices*, December 2011, available at www.oaic.gov.au.

Voluntary and self-regulatory guidance in the form of *The Australian Best Practice Guideline for Third Party Online Behavioural Advertising* (**OBA**) (the **Guideline**) (available at www.youronlinechoices.com.au) is generally observed as best practice with respect to the collection and use of data for the purpose of third party OBA. The Guideline recommends that online service providers engaging in third party OBA should obtain express consent from web users in relation to their collection and use of OBA data.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

See the response to question 7.5.

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

As at March 2017, neither ACMA nor the OAIC has taken any reported enforcement actions in relation to the use of cookies.

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

See the responses to questions 7.2 and 7.4 above.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad.

APP 8 regulates the cross-border disclosure of personal information to recipients outside of Australia.

Before disclosing personal information to an overseas recipient, APP 8.1 requires an APP entity to take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to that information.

In some circumstances, an act done, or a practice engaged in, by the overseas recipient that would breach the APPs, is taken to be a breach of the APPs by the disclosing entity (s 16C). This is commonly referred to as the 'accountability principle'. Generally, the accountability principle will apply where APP 8.1 applies to the disclosure, and the overseas recipient is not subject to the APPs, but the act or practice would be a breach of the APPs if they were. APP 8.2 lists a number of exceptions to APP 8.1 (and therefore to the operation of the accountability principle in s 16C). For example, APP 8.1 will not apply where:

- the entity reasonably believes that the recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is, overall, substantially similar to the APPs, and there are mechanisms available to the individual to enforce that protection or scheme (APP 8.2(a)); or
- an individual consents to the cross-border disclosure, after the entity informs them that APP 8.1 will no longer apply if they give their consent (APP 8.2(b)).

An overseas transfer of personal information to an overseas recipient may not be a 'disclosure' if the personal information at all times remains under the effective control of the APP entity. The Commissioner has drawn a distinction between limited and controlled access to information by an overseas recipient under conditions prescribed by the APP entity, which may in appropriate circumstances be a 'use' by the APP entity rather than a 'disclosure' to an overseas entity. This distinction will be important in relation to many outsourcing and offshoring arrangements, including cloud service or 'as-a-service' offerings.

This area of regulation is still developing and care should be taken to review and follow guidance issued by the Commissioner. See in particular OAIC *APP guidelines* chapter 8 and *Privacy business resource 8: Sending personal information overseas*.

Note, however, that some categories of personal information are subject to special or additional rules. Part IIIA of the Privacy Act regulates credit reporting and includes some restrictions on sending information held in the Australian credit reporting system overseas. The legislative framework for the Australian Government's My Health Record system prevents certain My Health Record operators and service providers from holding, taking, processing or handling records held for My Health Record purposes outside Australia, and from causing or permitting anyone else to do so. Some state and territory health privacy acts limit transfer of health information out of the relevant state or territory.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Typically, Australian companies will seek to satisfy the requirement of APP 8.1 by entering into an enforceable contractual arrangement with the overseas recipient (and any subcontractors) to handle the personal information in accordance with the APPs.

The Commissioner has stated that it is generally expected that an APP entity will enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the personal information in accordance with the APPs (other than APP 1), and further that it will take active steps to ensure compliance with those contractual arrangements.

The 'reasonable steps' test under APP 8.1 may also require an entity to take additional and more rigorous steps depending on the nature of the disclosure and, for example, the sensitivity of the information concerned. Such steps may include the imposition of audit rights to monitor the recipient's compliance with the terms of the contract and, by extension the APPs, in relation to the information.

With the introduction in March 2014 of the accountability principle (as embodied in section 16C of the federal Privacy Act), organisations may seek to rely on the exceptions to the general cross-border rule so as to avoid strict liability in relation to the breaches of the APPs by the overseas recipient. The scope and application of the exceptions are presently unclear and entities will need to be cautious in their reliance on them.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

The disclosure or transfer of personal information abroad does not require registration, notification or prior approval from the Commissioner.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

The Privacy Act does not regulate the scope of issues that may be reported via a whistle-blower hotline. The OAIC has not issued (as at March 2017) any guidance on the use of corporate whistle-blower hotlines in Australia.

The Australian *Corporations Act 2001* (Cth) (**Corporations Act**) establishes certain protections for corporate whistle-blowers. This includes protections for the confidentiality of information that the whistle-blower provides. Pursuant to sections 1317 AA-AE of the Corporations Act, a person is protected as a discloser if they are:

- an officer of a company;
- an employee of a company; or
- a contractor or their employee who has a contract to supply goods or services to the company.

The Corporations Act prohibits retaliation against a discloser and gives them a civil right, including seeking reinstatement of employment.

To qualify for protection, a whistle-blower's revelation must be made to:

- the Australian Securities and Investments Commission (**ASIC**);
- the company's auditor or a member of the audit team conducting an audit of the company;
- a director, secretary or senior manager;
- a senior manager of the company; or
- a person authorised by the company to receive disclosures of that kind. To trigger the provisions of the Corporations Act, the discloser must:
  - give their name before making the disclosure;
  - have reasonable grounds to suspect that the information indicates the company or an officer or employee has, or may have, contravened a provision of the corporations legislation; and
  - act in good faith.

Under the Corporations Act, information provided by a discloser and the identity of the discloser (or information that may lead to the identity of the discloser) may only be passed on under the following circumstances:

- without asking for the discloser's permission, to ASIC, the Australian Prudential Regulatory Authority or the Australian Federal Police; and
- to another person only if the discloser has given their consent.

Australian Standard *Whistle-blower Program for Entities, AS 8004-2003*, provides a guide to key requirements of a whistleblowing framework. Relevant requirements include confidentiality, anonymity and protection against negative action.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

The Privacy Act does not prohibit anonymous reporting. Under APP 2, entities must give individuals the option of engaging with them anonymously or pseudonymously unless it is impracticable or unlawful to do so. Entities would need to have regard to APP 2 in determining whether to permit anonymous reporting through a whistle-blower hotline.

Australian Standard *Whistle-blower Program for Entities, AS 8004-2003* at paragraph 2.3.5 states that a whistle-blower who reports or seeks to report reportable conduct should be given a guarantee of anonymity (if anonymity is desired by the whistle-blower) bearing in mind that in certain circumstances the law may require disclosure of the identity of the whistle-blower in legal proceedings.

However, a whistle-blower must identify him or herself by name when making a disclosure to the relevant person or authority to qualify for whistle-blower protections afforded by the Corporations Act.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

Corporate whistle-blower hotlines do not require separate registration/notification or prior approval from federal or state data protection authorities.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

Corporate whistle-blower hotlines do not require separate registration/notification or prior approval from federal or state data protection authorities.

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

Australian Standard *Whistle-blower Program for Entities, AS 8004-2003* at paragraph 2.3.4 states that an entity should have dedicated and highly visible alternative means for reporting reportable conduct. These alternative means should be well communicated to all employees, managers, contractors and other persons connected to the entity. However, there is no requirement for prior consultation.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No. The use of CCTV in Australia is regulated both at the federal and state level but this regulation is generally by way of requirements for notice to individuals subject to surveillance and, in some cases (notably, workplace surveillance), their consent.

The Privacy Act does not require an entity to register, notify or seek the prior approval of the Commissioner in relation to the use of CCTV.

Similarly, state surveillance legislation does not require an organisation to register, notify or seek the approval of state data protection authorities.

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

The use of CCTV by employer entities is regulated primarily on a state and territory basis by a mixture of workplace-specific and general surveillance legislation. See, for example, the *Workplace Surveillance Act 2005* (NSW), which regulates an employer's use of workplace surveillance in the state of New South Wales and the *Surveillance Devices Act 1999* (Vic), which governs the use of surveillance devices in general.

The *Workplace Surveillance Act 2005* (NSW) and the *Workplace Privacy Act 2011* (ACT) prohibits the surveillance by employers of their employees at work except where employees have been given notice or where the employer has obtained covert surveillance authority from a magistrate. These Acts regulate the surveillance of employees by way of camera, computer and tracking surveillance. Workplace monitoring by way of 'computer surveillance' (surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, the sending and receipt of emails)) requires:

- 14 days' prior notice to employees; and
- notice to each prospective employee before the prospective employee commences employment.

Computer surveillance clearly would include surveillance of workplace emails and instant messages.

The notice must indicate:

- the kind of surveillance to be carried out (camera, computer or tracking);
- how the surveillance will be carried out;
- when the surveillance will start;
- whether the surveillance will be continuous or intermittent;
- whether the surveillance will be for a specified limited period or ongoing;
- in the A.C.T., the purpose for which the employer may use and disclose the surveillance records; and
- in the A.C.T., that the employee may consult with the employer about the conduct of the surveillance.

In addition, computer surveillance of an employee must not be carried out unless:

- the surveillance is carried out in accordance with a policy of the employer on computer surveillance of employees at work; and
- the employee has been notified in advance of that policy in such a way that it is reasonable to assume that the employee is aware of and understands the policy.

The position in relation to monitoring of inbound emails or instant messaging sent from third party senders to employees is much less clear: some state statutes appear to require two party (sender and recipient) consent, others (Victoria, Queensland and the A.C.T.) allow one party to consent (sometimes referred to as a 'participant monitoring exception').

The *Surveillance Devices Act 1999* (Vic) regulates the use of listening, optical, tracking and data surveillance devices generally (whether used in a workplace or otherwise). Relevantly, the Act prohibits the installation, use or maintenance of optical surveillance devices to observe private activities without the express or implied consent of the individuals concerned.

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

Generally, employers may not engage in workplace surveillance without first providing notice to the affected employees: see further the response to question 10.2 above.

To the extent that such surveillance involves the collection of personal information for inclusion in a record, APP 5 of the *Privacy Act* would also require an entity to take reasonable steps to ensure that the employees were made aware of certain mandatory information, such as the purpose for which the information is collected.

Australian entities typically meet the notification requirements by providing prospective employees with notice through workplace agreements and associated policy documents. Under the *Workplace Surveillance Act 2005* (NSW), entities may provide notice by way of an email to the employee. Entities must also, however, place surveillance notices at each entrance to a workplace in which surveillance by camera occurs.

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

Neither federal nor state or territory surveillance laws require an entity to notify or consult with relevant trade unions or employee organisations in relation to the use of CCTV in the workplace.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No, it does not.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

An APP entity may process or store personal information in the cloud subject to the requirements of the Privacy Act and, where a cross-border 'disclosure' of personal information occurs, the cross-border restrictions are set out in APP 8. As noted above under question 8.1, there will not always be a 'disclosure' where offshore contractors are used but wherever there is such a disclosure, APP 8 requires an organisation to take reasonable steps to ensure that the overseas recipient (in this case, the overseas-based cloud provider) does not breach the APPs in relation to the information.

Accordingly, the requirement to take 'reasonable steps' in respect of the acts and practices of an overseas recipient of personal information may, depending on the particular cloud arrangements and in particular whether a relevant 'disclosure' occurs in respect of the cloud service provider, require an APP entity to undertake due diligence as to the cloud provider's privacy handling practices and the adequacy of existing technical and operational data security safeguards implemented by the provider. However, regardless of whether 'reasonable steps' were so taken, the Australian entity will generally remain accountable pursuant to section 16C in the event of any act or practice of a cloud service provider which, had it been undertaken by the disclosing Australian entity, would have been a breach of the APPs.

This area of regulation is still developing and care should be taken to review and follow guidance issued by the OAIC. See in particular OAIC *APP guidelines* chapter 8 and *Privacy business resource 8: Sending personal information overseas*.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The requirement in APP 8.1 to ensure that an overseas recipient does not breach the APPs is qualified by a 'reasonable steps' test. The Commissioner in APP guidelines chapter 8 states that it is generally expected that an APP entity will enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the personal information in accordance with the APPs (other than APP 1) and that contractual arrangements may include:

- the types of personal information to be disclosed and the purpose of disclosure;
- a requirement that the overseas recipient complies with the APPs in relation to the collection, use, disclosure, storage and destruction or de-identification of personal information. This should also require the overseas recipient to enter a similar contractual arrangement with any third parties to whom it discloses the personal information (for example, a subcontractor);

- the complaint handling process for privacy complaints; and
- a requirement that the recipient implement a data breach response plan which includes a mechanism for notifying the APP entity where there are reasonable grounds to suspect a data breach and outlines appropriate remedial action (based on the type of personal information to be handled under the contract).

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The Privacy Act does not preclude the use or disclosure of personal information in connection with big data and analytics. The Act is not prescriptive as to the due diligence that is required in these circumstances. Rather, the standard principles with respect to notification of collection (APP 5) and secondary purpose use and disclosure (APP 6) will apply to the use or disclosure of personal information for these purposes.

Entities proposing to use or disclose personal information for big data and analytics would also be subject to the requirements to take reasonable steps to ensure that they protect the information from (among other things) misuse, unauthorised modification and disclosure. Reasonable steps in this context may require an organisation to undertake due diligence to ensure that big data and analytics providers maintain sufficient technical and operational safeguards to protect personal information.

Effective de-identification of personal information, so that no individual is reasonably identifiable either from the information itself or other information available to that person, has the effect that the information ceases to be regulated as personal information. Many data analytic applications may be undertaken utilising de-identified information. The Commissioner will consider whether de-identification has been effective to mitigate re-identification risk 'in the round', that is, having regard to relevant facts and circumstances including limitations upon any subsequent use or disclosure of the de-identified information and any technical, operational and contractual safeguards against re-identification.

This area of regulation is still developing and care should be taken to review and follow guidance issued by the OAIC. In May 2016, the OAIC issued a consultation draft of *Guide to big data and the Australian Privacy Principles*. The closing date for submissions on this consultation was 26 July 2016 and as at the time of writing, the guide had not yet been finalised.

Pending finalisation of this guidance, the most relevant regulatory guidance is *Privacy business resource 4: De-identification of data and information*, available at https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business- resource-4-de-identification-of-data-and-information.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

The Privacy Act does not require APP entities to adopt particular data security standards. Rather, the Act (through APP 11) imposes a general obligation on entities to take such steps as are reasonable in the circumstances to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Accordingly, it is incumbent on each entity to determine what reasonable data security standards it must adopt to protect personal information given the circumstances of the particular act or practice. Such an exercise will include consideration of a range of factors, including the amount and sensitivity of the personal information concerned and the practicability and cost of the security measures contemplated.

The OAIC has published a *Guide to securing personal information* (January 2015), which sets out a range of 'reasonable steps' that may be adopted to protect personal information. The Guide can be found here: http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/Guide_to_securing_personal_information.pdf.

13.2 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) expects voluntary breach reporting.

On 13 February 2017, the Federal Parliament enacted the P*rivacy Amendment (Notifiable Data Breaches) Act 2017*, incorporating mandatory data breach notification requirements into the Privacy Act. These provisions will replace the voluntary data breach notification guidelines that are currently administered by the OAIC and require APP entities to notify both the Commissioner and affected individuals if the entity experiences an 'eligible data breach' that is a breach that a reasonable person would conclude is likely to result in serious harm to the individual/s concerned.

Limited exceptions to the notification requirements are available, including a public interest exception of avoiding prejudicing the activities of law enforcement agencies or disclosing information where it would be inconsistent with a secrecy provision in another law.

In the absence of an exception, where an entity has reason to suspect that an eligible data breach may have occurred, the entity is required to undertake a reasonable and expeditious assessment of the circumstances and in any event take all reasonable steps to complete that assessment within 30 days.

If an entity has reasonable grounds to believe they have experienced an eligible data breach, after an assessment or otherwise, the entity must notify the Information Commissioner and affected individuals. Reasonable grounds may be either direct evidence or indirect inference: for example, a pattern of complaints may provide the entity reasonable grounds to believe that an eligible data breach of the entity has occurred.

The form of notification to the Privacy Commissioner will be a 'subparagraph 26WK(2)(a)(i) statement'. Required information includes: the identity and contact details of the entity; a description of the eligible data breach that the entity has reasonable grounds to believe has happened; the kind or kinds of information concerned; and recommendations about the steps that individuals should take in response to the data breach. The recommendations are intended to provide individuals whose information has been compromised in an eligible data breach with general advice about steps they should take to mitigate the harm that may arise to them as a result: for example, recommending that individuals request a copy of their credit report if an eligible data breach might result in credit fraud.

The Commissioner will have power to investigate possible noncompliance with the mandatory data breach notification requirements and potentially make a determination requiring the entity to remedy such noncompliance. The Commissioner already receives frequent voluntary data breach notifications and has extensive experience in assessing such notifications. We may also expect new guidance from the Commissioner on the new mandatory requirements over forthcoming months.

The new provisions will be subject to a transitional regime and some requirements may not fully commence for 12 months after the Act commences operation. As at March 2017, it is not yet clear when the transition will be completed.

13.3 Is there a legal requirement to report data breaches to individuals? 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) expects voluntary breach reporting.

Yes – as described above, the new mandatory data breach notification regime requires notification to affected individuals, as well as the OAIC.

Notification of the contents of the subparagraph 26WK(2)(a)(i) statement (as described in the answer to question 13.2 above) must also be given to affected individuals. There are three alternative requirements or options, subject to 'practicability' (which involves consideration as to the time, effort or cost of a particular form of notification, when considered in all the circumstances of the entity and the data breach). An entity must either:

- if it is practicable to do so, take such steps as are reasonable in the circumstances to notify each of the individuals to whom the relevant information compromised in an eligible data breach relates;
- if it is practicable to do so, take such steps as are reasonable in the circumstances to notify those individuals who are considered to be 'at risk' of serious harm from the eligible data breach; or
- if it is not practicable to notify via either of the above two methods, notify affected individuals by publishing the statement on the entity's website and taking reasonable steps to publicise the statement. For example, if it is reasonable to do so, an entity could take out multiple print or online advertisements (which could include paid advertisements on social media channels), publish posts on multiple social media channels, or use both traditional media and online channels.

13.4 What are the maximum penalties for security breaches?

The Commissioner may determine a range of remedies for breaches of the APPs, including a declaration that compensation should be paid for any loss or damage suffered by the complainant. In addition, serious or repeated breaches of the APPs are punishable by civil penalties of up to AU$1.8 million.

The new mandatory data breach notification scheme described in the answers to questions 13.2 and 13.3 above is connected to the existing enforcement framework under the Privacy Act, such that the Privacy Commissioner's existing investigatory powers will apply in the event that an entity breaches a requirement of the notification scheme.

14 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
The power to investigate complaints about alleged interferences with the privacy of an individual.	The Commissioner may: ■ accept an enforceable undertaking; ■ bring proceedings to enforce an enforceable undertaking; ■ make a determination; ■ bring proceedings to enforce a determination; ■ seek an injunction including before, during or after an investigation or the exercise of another regulatory power; and/or ■ apply to the Court for a civil penalty order for a breach of a civil penalty provision.	This is not applicable in Australia.
The power to investigate (and to conduct preliminary inquiries to determine whether or not to investigate), on the Commissioner's own initiative, a breach of the Act.	As above. The Commissioner may also report to the Minister in certain circumstances following a Commissioner-initiated investigation.	This is not applicable in Australia.
The power to attempt to conciliate a complaint.	In limited situations, the Commissioner may accept an enforceable undertaking as part of the resolution of a complaint. Where conciliation is unresolved, the Commissioner may make a determination or decline to investigate the complaint further.	This is not applicable in Australia.
The power to obtain information and documents relevant to an investigation.	This is not applicable in Australia.	The failure to give information, answer a question or produce a document or record is punishable by a fine of up to AU$10,000 for a corporation.
The power to examine witnesses.	This is not applicable in Australia.	A failure to attend before the Commissioner, or swear or make an affirmation when required is punishable by a fine of up to AU$2,000 or imprisonment for 12 months, or both.

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
The power to direct a person to attend a compulsory conference.	This is not applicable in Australia.	A failure to comply with a direction to attend a conference is an offence punishable by a fine of up to AU$1,000 for individuals or imprisonment for a period of up to six months; in the case of a body corporate, a fine of up to AU$5,000.
The power to enter premises and inspect documents with consent or pursuant to a warrant.	This is not applicable in Australia.	This is not applicable in Australia.

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

Before 2014, the Commissioner had seldom exercised the power to make determinations as to an alleged breach of privacy. However, in the period between 2014 and 2017, the Commissioner made 19 determinations (with nine determinations made in 2016 alone) and an upward trend in formal enforcement activity appears to be continuing. That noted, in most cases, the Commissioner will seek to conciliate complaints between the relevant parties. An apology to the complainant is the most common remedy achieved through conciliation, followed by compensation. The amount of compensation paid between 2014 and 2017 varied between AU$2,000 to AU$20,000. As at March 2017, the Commissioner had awarded the largest sum of damages when it found that a respondent, in breaching the notification requirements for collection of personal information under APP 5 and the disclosure requirements under APP 6, had demonstrated "*a reckless indifference to the privacy rights of the complainant*" and awarding general damages of AU$15,000 and aggravated damages of AU$5,000. The Commissioner has also sought for the respondents to amend information handling procedures and to train staff in accordance with the revised procedures.

The Commissioner's enforcement powers include powers to:

- seek civil penalties against an organisation for serious or repeated interferences with the privacy of an individual (with penalties of up to AU$1.8 million for corporations); and
- accept enforceable undertakings as to a compliance with the Privacy Act.

As at March 2017, the Commissioner has accepted five enforceable undertakings. An enforcement undertaking may impose a significant administrative and operational load upon the party giving the undertaking. By way of example, following two information security breaches by Singtel Optus, in July 2014, the Commissioner initiated an investigation which concluded with the Commissioner agreeing to accept an enforceable undertaking from Singtel Optus. Optus undertook to:

- engage an independent auditor to conduct reviews and provide audit certifications, including as to whether Optus's practices, procedures and systems are reasonable to protect the personal information Optus holds from misuse, interference or loss, or unauthorised access, modification or disclosure; and whether enhancements to Optus's monitoring programme of change management that has the potential to affect the security of its customers' personal and sensitive information and as to Optus's penetration testing for fixed and mobile services were effective;
- conduct on an ongoing basis an audit review of new procedures for review of all major IT projects as part of Optus's Security Risk Assessment process and as part of its annual monitoring programme; and
- conduct a review of Optus's vulnerability detection processes across the organisation; certifications of a privacy incident review, a service level security posture assessment, an architecture review of Optus's principal IT systems (top 20 applying a risk-based approach), and a review of Optus' new voicemail platform.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Australian companies must handle requests for personal information from foreign law enforcement agencies or under foreign e-discovery requests in the same way as any other secondary purpose disclosure under the Act (see APP 6). In some cases, this may require the company to obtain the individual's consent to the disclosure unless another exception to the secondary disclosure prohibition is applicable.

Companies may also need to meet the requirements of APP 8 in relation to any cross-border disclosure of personal information to a foreign law enforcement agency or in response to a foreign e-discovery request.

In certain limited circumstances, Australian companies are permitted to disclose personal information:

- to law enforcement bodies for one or more enforcement related activities; or
- as required by, or authorised under, an Australian law or a court/tribunal order.

The enforcement bodies to which an organisation may disclose personal information are exhaustively defined in the Privacy Act and do not include foreign law enforcement agencies. Similarly, court/tribunal orders are limited to orders of an Australian court or tribunal and do not extend to foreign e-discovery requests.

15.2 What guidance has the data protection authority(ies) issued?

As at March 2017, the OAIC has not issued any guidance in relation to handling foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies.

16 Trends and Developments

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

As discussed in the response to question 14.2, the previous 12 months has seen an increase in the number of determinations made by the Commissioner.

There has also been an upward trend in the voluntary notification of data breaches to the OAIC.

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

The introduction of a mandatory data breach notification scheme has continued to be a key focus for the Commissioner and has now culminated in the incorporation of mandatory data breach notification requirements into the Privacy Act (see the answer to question 13.2 above). We may expect new guidance in relation to the scheme from the Commissioner over the forthcoming months.

On 19 January 2017, the Full Federal Court dismissed an application by the Commissioner seeking orders in relation to a decision by the Australian Administrative Appeals Tribunal, which had overturned a determination by the Commissioner granting the journalist, Ben Grubb, access to certain data relating to his use of Telstra mobile services. The Court's judgment usefully clarifies that the particular context of data collection and use is relevant to determination of whether information is 'personal information'. In this particular context (cell tower location and call usage information relating to a mobile phone), the device-related and network-related information sought by Mr. Grubb could be traced back to him as an 'identifiable individual', but was found by the Court not to be sufficiently related to him as to be information 'about that individual' protected as 'personal information' under the Privacy Act.

The Court's reasoning makes it clear that there are significant limits as to when device-related and network-related information is 'about an individual whose identity may be reasonably ascertained from the information' – a key issue that arises for many Internet of Things (IoT) applications now entering the market. However, and unfortunately, the Court failed to provide a methodology or useful guidance as to the point at which relevant information (including metadata) ceases to be 'about an individual'. So we remain unguided on this point.

The Australian Productivity Commission is currently completing a 12-month public inquiry into *Data Availability and Use*, which aims to investigate ways to improve the availability and use of public and private sector data. The Commission's draft report was released on 3 November 2016 (available at: http://www.pc.gov.au/inquiries/current/data-access#draft), and found that there is still enormous untapped potential in Australia's data and that better utilisation of it would benefit all Australians, particularly in the consumption of services in the finance and health sectors. The Commission proposed a draft data reform package aimed at moving Australia from a system based on risk aversion and avoidance, to one based on transparency and confidence in data processes, underpinned by four key elements: giving individuals more control over their data; enabling broader access to datasets of national interest; increasing the usefulness of publicly funded identifiable data; and creating a culture in which non-personal and non-confidential data is released by default. The Commission's final report is due imminently in the coming months.

Melissa Fai
Gilbert + Tobin
Level 35, Tower Two
International Towers Sydney
200 Barangaroo Avenue, Barangaroo
Sydney NSW 2000
Australia

Tel: *+61 2 9263 4685*
Email: *mfai@gtlaw.com.au*
URL: *www.gtlaw.com.au*

Melissa advises on complex outsourcing, IT and related procurement or supply transactions, from both a customer and supplier perspective, including IT transformation projects and business process outsourcing.

As part of her IT and commercial practice, Melissa also advises clients on privacy and data protection compliance obligations in relation to their commercial and marketing practices and data usage requirements.

She also has significant experience advising on the commercial and regulatory IT and data separation issues associated with strategic corporate transactions.

Alex Borowsky
Gilbert + Tobin
Level 35, Tower Two
International Towers Sydney
200 Barangaroo Avenue, Barangaroo
Sydney NSW 2000
Australia

Tel: *+61 2 9263 4182*
Email: *aborowsky@gtlaw.com.au*
URL: *www.gtlaw.com.au*

Alex is a lawyer in Gilbert + Tobin's TMT Group, advising Australia's largest corporations and government departments on a range of commercial projects with a focus on complex IT outsourcing, transformation, data protection and privacy.

As part of her IT and commercial practice, Alex advises clients on privacy, data protection and regulatory compliance obligations in relation to their commercial and marketing practices, technology platforms and digital strategies. She also has significant experience advising on cross-border transfers of personal information, information security and dealings with the Privacy Commissioner and other law enforcement agencies.

Gilbert + Tobin is an independent Australian corporate law firm. We serve corporates and governments throughout Australia, and around the world, on a broad range of legal issues.

We are renowned for our progressive approach to legal issues, procedures and client service. From our Sydney, Melbourne and Perth offices, our lawyers bring a proactive, commercial approach, and a relentless drive to deliver superior results.

Founded as a disruptive startup in 1988, we have built a firm with the scope to take on the tough matters. We cut through complexity – helping clients make the right decision in the most effective way.

Other titles in the ICLG series include:

- Alternative Investment Funds
- 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
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International 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 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