The International Comparative Legal Guide to:
Data Protection 2014
1st Edition
A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

BANNING
Barrera, Siqueiros y Torres Landa, S.C.
CMS Reich-Rohrwig Hainz
Dittmar & Indrenius
DLA Piper
ECIJ ABOGADOS
Eversheds
Gilbert + Tobin Lawyers
Herbst Kinsky Rechtsanwalte GmbH
Hunton & Williams
KALO & ASSOCIATES
Koep & Partners

Marrugo Rivera & Asociados, Estudio Jurídico
Matheson
Mori Hamada & Matsumoto
Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados
Osler, Hoskin & Harcourt LLP
Pachi & Associates
Pestalozzi
Portolano Cavallo Studio Legale
Raja, Darryl & Loh
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA
General Chapter:

1 Data Protection – a Key Business Risk – Bridget Treacy, Hunton & Williams

Country Question and Answer Chapters:

2 Albania KALO & ASSOCIATES: Eni Kalo
3 Australia Gilbert + Tobin Lawyers: Peter Leonard & Ewan Scobie
4 Austria Herbst Kinsky Rechtsanwälte GmbH: Dr. Sonja Hebenstreit & Dr. Isabel Funk-Leisch
5 Belgium Hunton & Williams: Wim Nauwelaerts & Laura De Boel
6 Brazil Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados: Renato Opice Blum
7 Canada Osler, Hoskin & Harcourt LLP: Adam Kardash & Bridget McIlveen
8 China Hunton & Williams LLP Beijing Representative Office: Manuel E. Maisog & Zhang Wei
9 Colombia Marrugo Rivera & Asociados, Estudio Jurídico: Ivan Dario Marrugo Jimenez
10 Finland Dittmar & Indrenius: Jukka Lång & Iiris Keino
11 France Hunton & Williams: Claire François
12 Germany Hunton & Williams: Dr. Jörg Hladjk & Johannes Jördens
13 India Subramaniam & Associates (SNA): Hari Subramaniam & Aditi Subramaniam
14 Ireland Matheson: John O’Connor & Anne-Marie Bohan
15 Italy Portolano Cavallo Studio Legale: Laura Liguori & Federica De Santis
16 Japan Mori Hamada & Matsumoto: Akira Marumo & Hiromi Hayashi
17 Kosovo KALO & ASSOCIATES: Loriana Robo & Atdhe Dika
18 Malaysia Raja, Darryl & Loh: Tong Lai Ling & Roland Richard Kual
19 Mexico Barrera, Siqueiros y Torres Landa, S.C.: Mario Jorge Yanez V. & Federico de Noriega O.
20 Namibia Koep & Partners: Hugo Meyer van den Berg & Chastin Bassingthwaighte
21 Netherlands BANNING: Monique Hennekens & Chantal Grouws
22 New Zealand Wigley & Company: Michael Wigley
23 Norway Wikborg, Rein & Co. Advokatfirma DA: Dr. Rolf Riisnæs & Dr. Emily M. Weitzenboeck
24 Romania Pachiu & Associates: Mihaela Cracea & Ioana Iovanesc
25 Slovenia CMS Reich-Rohrhwald Hainz: Luka Fabiani & Ela Omersa
26 South Africa Eversheds: Tanya Waksman
27 Spain ECUJA ABOGADOS: Carlos Pérez Sanz
28 Switzerland Pestalozzi: Clara-Ann Gordon & Dr. Michael Reinle
29 United Kingdom Hunton & Williams: Bridget Treacy & Naomi McBride
30 USA DLA Piper: Jim Halpert & Kate Lucente
EDITORIAL

Welcome to the first edition of *The International Comparative Legal Guide to: Data Protection*.

This guide provides the international practitioner and in-house counsel with a comprehensive worldwide legal analysis of the laws and regulations of data protection.

It is divided into two main sections:

One general chapter entitled *Data Protection – a Key Business Risk*.

Country question and answer chapters. These provide a broad overview of common issues in data protection laws and regulations in 29 jurisdictions.

All chapters are written by leading data protection lawyers and industry specialists and we are extremely grateful for their excellent contributions.

Special thanks are reserved for the contributing editor Bridget Treacy of Hunton & Williams for her invaluable assistance.

Global Legal Group hopes that you find this guide practical and interesting.

The *International Comparative Legal Guide* series is also available online at www.iclg.co.uk.

Alan Falach LL.M.  
Group Consulting Editor  
Global Legal Group  
Alan.Falach@glgroup.co.uk
Chapter 3

Australia

Gilbert + Tobin Lawyers

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, Australian Capital Territory (ACT) government agencies and private sector organisations. Pursuant to a ‘small business exception’ and with important qualifications, generally private sector organisations are only regulated where their annual Australian revenue is greater than AUD$3 million.

The Privacy Act includes:

- 13 Australian Privacy Principles (APPs) which apply to the handling of personal information by government agencies and private 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));
- 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 Tax File Number Guidelines 2011 issued under the Privacy Act also regulate the collection, storage, use, disclosure, security and disposal of individuals’ TFN by public agencies and private organisations;
- Spam Act 2003 (Cth), which deals with the sending of unsolicited commercial electronic messages, including emails and SMS;
- Do Not Call Register Act 2006 (Cth), regulating unsolicited commercial calling to telephone numbers listed on the national Do Not Call Register;
- federal and state and territory laws governing telecommunications interception and the use of listening devices and workplace surveillance and/or unauthorised video surveillance; and
- federal and state criminal laws dealing with unauthorised access to computer systems.

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:

- Healthcare Identifiers Act 2010 (Cth), regulating (among other things) the use and disclosure of healthcare identifiers;
- 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; and
- Personally Controlled Electronic Health Records Act 2012 (Cth), which provides strict controls on the collection, use and disclosure of health information included in an individual’s eHealth record.

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; and
- 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.

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

The Privacy Act is administered by the Australian Privacy Commissioner which is integrated within the Office of the Australian Information Commissioner (OAIC). The OAIC is responsible for enforcing compliance with the Privacy Act and reviewing proposed privacy codes.

The Australian Communications and Media Authority (ACMA)
also plays an active role in regulating and enforcing privacy-related legislative schemes. For example, the ACMA enforces the provisions of the Spam Act and the Do Not Call Register Act. State and territory data protection commissioners are responsible for ensuring compliance with relevant legislation by state and territory government agencies.

2 Definitions

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

- **“Personal Data”**
  ‘Personal Information’ means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.

- **“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;
  - 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.

- **“Data Controller”**
  The term ‘data controller’ is not used in the Privacy Act. Organisations and Government agencies that collect, use or disclose personal information are called ‘APP entities’.

- **“Data Processor”**
  The term ‘data processor’ is not used in the Privacy Act.

- **“Data Owner”**
  The term ‘data owner’ is not used in the Privacy Act.

- **“Data Subject”**
  The term ‘data subject’ is not used in the Privacy Act. The Act refers to ‘individuals’ to which personal information relates.

- **“Pseudonymous Data”**
  The Privacy contains no definition for the term ‘Pseudonymous Data’.

- **“Direct Personal Data”**
  The Privacy Act contains no definition for the term ‘direct personal data’.

- **“Indirect Personal Data”**
  The Privacy Act contains no definition for the term ‘indirect personal data’.

Other key definitions

- **“APP entity”** means a government agency or private sector organisation.

- **“Australian Link”** an organisation or small business where the 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.

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.

- **Lawful basis for processing**
  The Privacy Act governs the collection, holding, use, disclosure, access and correction of personal information separately and does not refer to the concept of “processing”. The Act, however, 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.

- **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;
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
If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information. 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
In accordance with APP 13, if an APP entity holds personal information about an individual; and either the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or the individual requests the entity to correct the information, the entity must take such steps as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

We note deletion is covered under ‘Retention’ in question 3.1.

Objection to processing
As stated above, the European concept of “processing” is not applicable in Australia. Individuals may, however, withdraw their consent (if any) to the use of their personal information by an APP entity.

Objection to 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 conditions relating to provision of a convenient opt-out mechanism are met by the organisation.

The Spam Act 2003 and the Do Not Call Register Act 2006 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 email. It is unclear whether unsolicited promotional postings to social media pages may be ‘messages’ that are regulated as ‘spam’. The Do Not Call Register Act 2006 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 Do Not Call Register. 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 these other Acts. It follows that each of these Acts 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, however, 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 Privacy 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
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.

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 in Australia.

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 in Australia.

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 in Australia.

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

This is not applicable in Australia.

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

This is not applicable in Australia.

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

This is not applicable in Australia.

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

This is not applicable in Australia.

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

This is not applicable in Australia.

6 Appointment of a Data Protection Officer

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

The Privacy Act does not expressly require an APP entity to appoint a data protection officer. APP 1 does, however, require 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 many steps an entity can take to meet this obligation.

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.

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

This is not applicable in Australia.

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 formulating an APP entity’s privacy compliance strategy. This may entail designing and facilitating staff privacy training, 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)?

This is not applicable in Australia.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, e-mail, 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 2003 (Cth), which governs most forms of electronic marketing, and the Do Not Call Register Act 2006 (Cth), which regulates unsolicited telemarketing calls. APP 7 of the Privacy Act also plays a part in regulating the use or disclosure of personal information for the purpose of direct marketing activities. 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 implied in the circumstances), and if the message contains accurate sender identification and functional unsubscribe facility.

Voice calls, including synthetic or recorded calls (such as robocalls), are separately regulated under a ‘do not call’ regulatory framework established under the Do Not Call Register Act and associated legislation and instruments, including the Telecommunications (Do Not Call Registers) (Telemarketing and Research Calls) Industry Standard 2006. Marketing faxes are regulated under the Do Not Call Register Act. This Act provides an ‘opt-out’ framework for these forms of marketing. Unsolicited telemarketing calls or faxes must not be made to an Australian number registered on the Do Not Call Register.

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

The ACMA is active in enforcing the provisions of the Spam Act and the Do Not Call Register Act. 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 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.

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

The maximum penalty for two or more contraventions of the Spam Act or Do Not Call Register Act by a corporation (with no prior record) is $340,000.

The federal Privacy 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 $1.7 million.

### 7.4 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.

Voluntary and self-regulatory guidance in the form of the Australian Guideline for Third Party Online Behavioural Advertising (OBA) (the Guideline) 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.

### 7.5 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 7.4.

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

As of February 2013, the federal Privacy Commissioner has not taken any enforcement action in relation to cookies.

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

This is not applicable in Australia.

### 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 the accountability principle). 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)).

**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. APP 8.1’s ‘reasonable steps’ test 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 recipients’ compliance with the terms of the contract and, by extension the APPs, in relation to the information.

With the introduction of the new accountability principle, 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.

The disclosure or transfer of personal information abroad does not require registration, notification or prior approval from the federal Privacy 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 hotline. The OAIC has not issued (as from February 2014) any guidance on the use of corporate whistle-blower hotlines in Australia.

The Australian Corporations Act 2001 (Cth) establishes certain protections for corporate whistle-blowers. This includes protections for the confidentiality of information the whistle-blower provides. These legislative protections relate to good-faith disclosures of alleged breaches of the Corporations Act or the Australian Securities and Investments Commission Act 2001.

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.

Relevantly, a whistle-blower must identify him or herself by name when making a disclosure to the relevant person or authority to merit the 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.

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 federal Privacy Act does not require an entity to register, notify or seek the prior approval of the Privacy 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) 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. The Act regulates the surveillance of employees by way of camera, computer and tracking surveillance. Further, the Act expressly prohibits surveillance in a changing room, toilet facility or shower or other bathing facility at a workplace.

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.

To the extent that such surveillance involves the collection of personal information for inclusion in a record, APP 5 of the federal Privacy Act would 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.

Under the New South Wales Workplace Surveillance Act 2005 (NSW), an employer must not commence workplace surveillance without prior notice in writing to the employees concerned. Such notice must generally be given at least 14 days before the surveillance commences or before the employee starts work.

Australian entities typically meet the notification requirements by
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 set out in APP 8. As noted above under question 8.1, 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 disclosee 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 in the event of any act or practice of a cloud service provider which is undertaken by the Australian entity would be a breach of the APPs.

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 Privacy Act does not generally require an APP entity to impose specific contractual obligations on a processor providing cloud-based services. However, entities typically comply with the requirement to take ‘reasonable steps’ in APP 8.1 by entering into enforceable contractual arrangements with the provider to comply with the APPs in relation to the storage and processing of personal information.

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 collection notification (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.

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 federal 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 Office of the Australian Information Commissioner has published a Guide to information security (April 2013), 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/privacy/privacy-resources/privacy-guides/guide-to-information-security.

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.

As of February 2014, the Privacy Act does not impose obligations on organisations to notify either the OAIC, or the individual
Concerned, of data breaches involving personal information. However, the OAIC recommends notification and has published Guidelines in this area: *Data Breach Notification: A guide to handling personal information security breaches* (April 2002). Under the OAIC’s voluntary notification guidelines, the OAIC recommends notification of a data breach if it creates a real risk of serious harm to the individual/s concerned.

In 2013, the Australian Government introduced the Privacy Amendment (Privacy Alerts) Bill 2013, which provided for the establishment of a mandatory data breach notification scheme. However, the Bill lapsed due to the calling of the 2013 federal election and has not been reintroduced by the new Government (as of February 2014).

### 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.

See the answer to question 13.2 above.

### 14 Enforcement and Sanctions

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

<table>
<thead>
<tr>
<th>Investigatory/Enforcement Power</th>
<th>Civil/Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>The power to investigate complaints about alleged interferences with the privacy of an individual.</td>
<td>This is not applicable in Australia.</td>
<td>This is not applicable in Australia.</td>
</tr>
<tr>
<td>The power to investigate, on the Commissioner’s own initiative, a breach of the Act.</td>
<td>This is not applicable in Australia.</td>
<td>This is not applicable in Australia.</td>
</tr>
<tr>
<td>The power to obtain information and documents relevant to an investigation.</td>
<td>This is not applicable in Australia.</td>
<td>The failure to give information, answer a question or produce a document or record is punishable by a fine of up to $10,000 for a corporation.</td>
</tr>
<tr>
<td>The power to examine witnesses.</td>
<td>This is not applicable in Australia.</td>
<td>A failure to attend before the Commissioner, or swear or make an affirmation when required is punishable by a fine of up to $2,000 or imprisonment for 12 months, or both.</td>
</tr>
<tr>
<td>The power to direct a person to attend a compulsory conference.</td>
<td>This is not applicable in Australia.</td>
<td>A failure to comply with a direction to attend a conference is guilty of an offence punishable by a fine of up to $1,000 for individuals or imprisonment for a period of up to 6 months; in the case of a body corporate, a fine of up to $5,000.</td>
</tr>
</tbody>
</table>

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

The federal Privacy Commissioner has, to date, seldom exercised the power to make determinations as to an alleged breach of privacy. In the period 2012-2013, the Commissioner made only one determination in the matter of ‘S’ and Veda Advantage Information Services and Solutions Limited. In this matter, the Commissioner declared that the respondent apologise in writing to the complainant, undertake various other actions in relation to ensuring the integrity of the personal information contained in the complainant’s credit file, and pay the complainant $2,000 in compensation.

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 is relatively low and is, in the majority of cases, no more than $1,000.

From 12 March 2014, the Commissioner will receive significant new enforcement powers, including the power to:

- seek civil penalties against an organisation for serious or repeated interferences with the privacy of an individual (with penalties of up to $1.7 million for corporations); and
accept enforceable undertakings as to a compliance with the Privacy Act.

It is anticipated that the Commissioner will make active use of these new powers in future enforcement action.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within Australia 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 of February 2014, the OAIC has not issued any guidance in relation to handling foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies.

Acknowledgment

The authors would like to acknowledge the assistance of their colleague Michael Burnett in the preparation of this chapter.

Peter Leonard
Gilbert + Tobin Lawyers
Level 37
2 Park Street
Sydney NSW 2000
Australia
Tel: +61 2 9263 4003
Fax: +61 2 9263 4111
Email: pleonard@gtlaw.com.au
URL: www.gtlaw.com.au

Peter heads Gilbert + Tobin’s Internet, Media and Data Protection practice. His primary focus is commercial and corporate transactions and structuring for corporations active in the technology, media, communications and internet business fields. He is ranked as a leading lawyer in all major legal directories and was voted the communications industry’s Communications Ambassador of the Year 2012/13 for his contribution to the Australian communications industry. Peter chairs the Law Council of Australia’s Media and Communications Committee and he is also a director of the International Association of Privacy Professionals Australia and New Zealand (iappANZ).

Ewan Scobie
Gilbert + Tobin Lawyers
Level 37
2 Park Street
Sydney NSW 2000
Australia
Tel: +61 2 9263 4473
Fax: +61 2 9263 4111
Email: escobie@gtlaw.com.au
URL: www.gtlaw.com.au

Ewan advises on a broad range of regulatory and commercial media and communications matters, particularly in the fields of privacy, consumer protection and online regulation. Ewan also has experience in Intellectual Property working on commercial and litigious matters across the fields of copyright, patents and trade marks.

Gilbert + Tobin Lawyers

Gilbert + Tobin is a leading independent corporate law firm and a key player in the Australian legal market. From our Sydney, Melbourne and Perth offices, we provide innovative, relevant and commercial legal solutions to major corporate and government clients across Australia and internationally, particularly in the Asia-Pacific region.

Gilbert + Tobin’s reputation for expert advice extends across a broad range of areas including: TMT and project services; banking and finance; corporate advisory - funds, mergers and acquisitions, private equity, capital markets, tax and stamp duty; competition and regulation; energy and resources; intellectual property; media; litigation and dispute resolution; and real estate and projects.

Established in 1988, Gilbert + Tobin is now one of Australia’s largest independent law firms, employing more than 500 people. Throughout our growth we have had the highest proportion of female partners of any major Australian law firm. We are acknowledged as a pioneer in providing pro bono services, with a particular focus on indigenous Australians.
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 Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Environment & Climate Change Law
- Franchise
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Patents
- Pharmaceutical Advertising
- Private Client
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet