Ensuring Your Workplace Policies and Procedures Conform

A paper to be presented on 19 June 2014

Protecting Privacy: Checklist for Business Seminar, Brisbane

Authors
Alistair Macpherson, Director, Corney & Lind Lawyers
alistair.macpherson@corneyandlind.com.au
Nina Brewer, Lawyer, Corney & Lind Lawyers
nina.brewer@corneyandlind.com.au

Level 4, Royal Brisbane Place
17 Bowen Bridge Rd Herston Q 4029
Phone: (07) 3252 0011
Fax: (07) 3257 7890
www.corneyandlind.com.au

1 INTRODUCTION

1.1 Privacy law is the law around the collection, storage and use of personal information about individuals by government agencies and businesses. It is primarily governed by the *Privacy Act 1988* (Cth) ("**the Act**"). This Act has recently been the subject of extensive amendments, most notably the introduction of the Australian Privacy Principles.

1.2 Companies with an annual turnover of more than $3 million per annum are subject to the regulations imposed by the Act. Therefore, most workplaces will need to consider and if necessary, review their policies and procedures to ensure compliance with the Act.

1.3 This paper will address some main elements that Companies should consider and ensure compliance with.

2 HOW YOUR WORKPLACE POLICIES AND PROCEDURES SHOULD CONFORM

2.1 Management of Employee data: sharing data within organisational groups

Does the Act apply?

2.1.1 When sharing data within an organisational group, the primary consideration is whether the Act applies to the group. If it doesn't, then the management of personal information will be exempt from the scope of the Act. This will require an analysis of the group structure and the relationship of the entities.

2.1.2 Where entities are related, they are considered as a "whole" for the purposes of the economic turnover threshold for application of the Act. Section 6C of the Act exempts "small business operators" from the definition of an organisation to which the Privacy

Act applies. A “small business” is defined in section 6D(1) as a business who’s annual turnover is less than $3 million. However, even if a business is a small business, section 6D(9) of the Act states that:

> *... a body corporate is not a small business operator if it is related to a body corporate that carries on a business that is not a small business*.

Therefore, it is important to consider whether the business is a related body corporate to any entity with an annual turnover of more than $3 million. If it is, the Act applies to both entities.

2.1.3 Additionally, some small businesses can still be caught, if:

a They provide a health service;

b They disclose personal information about another individual to anyone else for a benefit, service or advantage;

c They provide a benefit, service or advantage to collect personal information about an individual;

d They are a contracted service provider for a Commonwealth Contract; or

e They are a credit reporting body.

Related Bodies Corporate

2.1.4 The term “related body corporate” is not defined in the Act. However, guidance can be taken from section 50 of the *Corporations Act 2001* (Cth), which states that:

> *“Where a body corporate is:*
>
> *(a) A holding company of another body corporate; or*
> *(b) A subsidiary of another body corporate; or*
> *(c) A subsidiary of a holding company of another body corporate;*
>
> *the first-mentioned body and the other body are related to each other.”*

2.1.5 As previously mentioned, the first step is to consider the relationship of the entities. The second step, if necessary, is to consider the impact that the Act has on the sharing of employee data between those entities.

Employee Records

2.1.6 In order to share employee data, the data itself must come within the scope of the Act.

2.1.7 Even if a corporation itself falls within the scope of the Privacy Act, certain Employee records are nevertheless exempt from the scope of the Privacy Act. This is known as the “employee records exemption”.

2.1.8 Section 7B(3) states that an act done, or a practice engaged in, by an organisation that is or was the employee’s employer is exempt from the scope of the Act if:

a the record is directly related to a current or former employment relationship; and

b the record is held by the Employer and is about their Employee.

Such an “act” will include the disclosure and collection of the employee record.

2.1.9 Section 6 of the Act defines an employee record as “*a record of personal information relating to the employment of the employee*”. It includes:

a the engagement, training, disciplining or resignation of the employee;

b the termination of the employment of the employee;

c the terms and conditions of employment of the employee;

d the employee's personal and emergency contact details;

e the employee's performance or conduct;

f the employee's hours of employment;

g the employee's salary or wages;

h the employee's membership of a professional or trade association;

i the employee's trade union membership;

j the employee's recreation, long service, sick, personal, maternity, paternity or other leave;

k the employee's taxation, banking or superannuation affairs.

Personal Information or Employee record?

2.1.10 The next thing to consider is whether the Employee record is being dealt with by the Employer, or by a different related entity. If it is by a different entity, it can no longer be considered to be an employee record and is subject to the Act as per the definition of personal information. This is where the definition of the “related bodies corporate” comes into play.

2.1.11 In relation to personal information, section 13B of the Act states that disclosure to, and collection from, a related body corporate is not an interference with the privacy of an individual. Essentially, this section allows related bodies corporate to share information. This is known as the “related bodies corporate exemption”. However, in holding or using the information, the related body corporate must comply with the APPs of a registered APP code that binds them.

2.1.12 The Act goes further to state in this section that the related bodies corporate exemption does not, however, apply where disclosure to the related body corporate is an exempt practice under the Act. The act of disclosure of an employee record falls within the “employee records” exemption contained within the Act.

2.1.13 By way of these two sections, these being the “related bodies corporate” exemption and the “employee records” exemption, bodies corporate are able to share all information that is not sensitive information.

2.1.14 However, it is our view that even if an entity is a “related body corporate” to another entity, they are nevertheless individually incorporated separate legal entities, and separately employ their own Employees. That is, the Employees of one company are not the Employees of that company’s related body corporate.

2.1.15 Once an employee record is shared between related bodies corporate, it then ceases to be an employee record (when held by the related body corporate).

2.1.16 It seems to us that upon receipt by the external entity or related body corporate, the information is considered to be personal information about an individual rather than an Employee record. It is, from that point, subject to the Act.

Australian Privacy Principles

2.1.17 I will now consider the main obligations with which the recipient related body corporate organisation must comply when using or disclosing Employee information.

2.1.18 APP 6 states that:

> *If an APP entity holds personal information about an individual that was collected for a particular purpose (the **primary purpose**), the entity must not use or disclose the information for another purpose (the **secondary purpose**) unless:*
>
> > *(a) the individual has consented to the use or disclosure of the information...*

2.1.19 That is, the personal information must be used for the primary purpose for which it was collected, unless an exception applies.

2.1.20 APP 6.6 directly addresses the "purpose" of the disclosure of personal information to related bodies corporate. It states that:

> *If:*
>
> *(a) An APP entity is a body corporate; and*
> *(b) The entity collects personal information from a related body corporate;*
>
> *[APP 6] applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.*

2.1.21 Therefore, there is a presumption that the related body corporate will utilise the Employee record for the same primary purpose as the Employee's Employer. Related bodies corporate must ensure that the purpose for which they use or disclose the personal information is the same purpose as the Employee's Employer.

2.2 Monitoring workplace use of internet and emails

2.2.1 Employee use of emails and the Internet has put the privacy rights of Employees under examination. Employees have an expectation of a degree of privacy at work. But does this extend to their reasonable use of emails and Internet for personal reasons?

2.2.2 The privacy implications of the use of email and Internet at work have not been specifically included in the scope of the Act, nor are they otherwise legislated.

2.2.3 Monitoring the use of workplace emails and Internet is a type of surveillance in the workplace. They can be easily monitored by Employers. However, the legislative framework regulating the monitoring of these types of technology has not yet been drafted.

2.2.4 There is currently no legislation expressly forbidding an Employer from monitoring workplace email usage, provided that the email server is owner by the Employer.

2.2.5 As a result of the *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* (Cth), emails stored on company hard drives, servers and other storage devices are no longer subject to the prohibition upon Employers against interception of communications passing over a telecommunications systems. That is, Employers may monitor emails. These amendments remove stored communications from the scope of restrictions placed upon Employers in relation to lawfully obtained information.

2.2.6 However, Employers must still carefully consider the nature and use of the information acquired through email monitoring. Workplace surveillance such as checking Employee email and Internet usage may constitute the collection and handling of personal information about the Employee concerned.

2.2.7 Informing people about the personal information that is collected, held and what is done with it is an important privacy principle. The Privacy Commissioner encourages organisations to develop in consultation with staff a clear privacy policy in relation to staff use of computer networks, particularly with regard to the use of e-mail and the Internet. It is recommended that the policy clearly set out the proper and permitted use of the network, including Internet e-mail and web browsing. This policy may form part of a general IT usage policy or a separate privacy policy dealing with e-mail and Internet use. Such an approach is likely to result in a policy that staff understand and accept.

2.2.8 The Policy should:

a Be placed in a position where it will be read, known and understood by Employees;

b Be very clear about which email and Internet-related activities are permitted, and which are forbidden;

c Be very clear about what information is recorded and "logged", and which members of staff will have the authority to access those records and logs;

d Outline very clearly exactly how the Company intends to monitor staff usage of emails and Internet;

e Be regularly reviewed to comply with changing technology.

2.3 Use of surveillance systems to monitor the workforce

2.3.1 The presence of CCTV surveillance systems in the workplace raises a whole range of issues, including balancing whether such surveillance is an invasion of Employees' privacy, against the Employer's interest in protecting their property and protecting themselves against being the victims of fraudulent activities conducted by their Employees.

2.3.2 I will be discussing the law surrounding CCTV surveillance systems in the Queensland jurisdiction only. Please note that other States and Territories differ significantly in their surveillance laws. There is no uniform legislation.

2.3.3 The Privacy Act does not specifically cover the use of workplace surveillance. New South Wales and the Australian Capital Territory are the only jurisdictions that have legislation specifically covering workplace surveillance. Both pieces of legislation impose strict standards, such as giving notice and obtaining permission from Employees, with which an Employer must comply when using covert surveillance devices.

2.3.4 The types of surveillance that may be used include:

a Optical video (CCTV);

b Listening devices;

c Telephone; and

d Computer monitoring. We have already covered this point.

2.3.5 Queensland relies generally on the common law regarding surveillance issues.

2.3.6 The Office of the Information Commissioner's guidelines to APP 3 state specifically that CCTV footage that identifies individuals is a type of **solicited personal information**. I note that this guideline pertains to the *content* of the surveillance footage, and not the legality of the act of recording the footage.

2.3.7 APP 3 regulates the collection of both personal information and sensitive information. For the purpose of CCTV footage, Employees need only consider the regulations around the collection of solicited personal information.

2.3.8 An entity "solicits" personal information where an entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included" (*Privacy Act 1988* (Cth) section 6(1)).

2.3.9 It naturally follows, however, that this information cannot be solicited, or be requested by an Employee of an Employer to provide that information, or participate in the CCTV footage, if the Employee is unaware that they are being monitored. Employers should therefore notify Employees of the fact that they under surveillance, or display signs around the workplace to that effect. This method is also consistent with the current legislation enforced in other States in specific relation to CCTV surveillance.

2.3.10 An exception to this is where the Employer needs to do covert recording, to respond to a particular issue of concern, such as suspected theft.

2.3.11 As the Commissioner's guidelines state that CCTV footage satisfies this definition of solicited personal information, it is not necessary to further justify the inclusion of that type of monitoring within the definition of solicited personal information.

2.3.12 It should also be noted that the collection of CCTV footage of Employees does not fall within the scope of the definition of "Employee record" and is thus subject to the authority of the Act.

2.3.13 APP 3 deals with two aspects of the collection of solicited personal information – *when* the information can be collected and *how* it can be collected.

2.3.14 To define when it may be collected, APP 3.2 states:

If an APP entity is an organisation, the entity 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.

This involves a two-step process - Identifying the entity's functions or activities, and determining whether the collection of the CCTV footage was reasonably necessary for one of those functions or activities.

a Identifying an entity's functions or activities

i This includes its current functions and activities, proposed functions and activities and other functions and activities that carries out in support of its other functions or activities (such as public relations).

b Determining whether the collection of information is "reasonably necessary" for one of those functions or activities

i The "reasonably necessary" test is determined objectively – that is, whether a reasonably person who is adequately informed would agree that the collection is necessary. The onus is on the Employer to prove that the collection was or is necessary.

ii Things that Employers should consider when collecting CCTV footage are:

A The main reason the Employer is collecting the footage;

B How the CCTV footage will be used in undertaking the function or activity of the entity;

C Whether the entity could undertake the function or activity without collecting the footage.

iii The Employer's duty of care to its Employees and clients that enter its premises is consistent with the running of a business and, for example, the provision of services to clients. As such, an Employer would be able to justify the use of CCTV surveillance cameras for the primary purpose of providing services to clients. The Employees and clients must, however, be aware of the use of these facilities. An appropriate way to create such awareness is to display signs to this effect in prominent places of the premises.

2.3.15 To define how it may be collected, APP 3.5 and 3.6 state that the information must be collected:

a By lawful and fair means;

i The term "lawful" is not defined in the Act, however requires the Employer to comply with legislation when collected the information as well as common law (such as not trespassing on private property to do so or by committing another civil wrong).

ii To collect by "fair means" is not to collect by intimidation or deception. Fair means would ordinarily require notifying individuals that they are being monitored by CCTV surveillance equipment unless there is a legitimate reason for not making this disclosure.

2.4 Privacy policies

2.4.1 I will not outline the intricacies of the elements that must be included within a Company's privacy policy. As a general overview, the requirements surrounding Privacy Policies are codified in APP 1.1 – 1.6 of the Act.

2.4.2 APP 1.4 provides a non-exhaustive list of information that an APP entity must include in its Privacy Policy:

a The kind of information collected and held (1.4(a)).

b How the personal information is collected and held (1.4(b)). For example, whether it is collected directly from the individual, or from referrals from other entities. It should also include how the personal information is stored (for example, if the information is held by a third party data storage providor). It should also state how the information is secured. However, the description of security measures should not jeopardise the effectiveness of those measures;

c The purposes for which the information is collected, held, used and disclosed (1.4(c));

d How an individual may access personal information about the individual that is held by the Company, and how an individual may seek the correction of that information (1.4(d)). As a minimum, the policy must state:

i That individuals have a right to access their personal information and request its correction (per APPs 12 and 13); and

ii The position title, telephone number, postal address and email address of the contact person for requests to access and correct personal information;

e How an individual may complain about a perceived breach of the APPs or a registered APP code, and how the Company will deal with such a complaint (1.4(e)). This must include the procedure for how an individual may complain, and the contact details of the person to whom the complaint is to be made in the first instance;

f Whether the entity is likely to disclose personal information to overseas recipients (1.4(f)), and if so, the countries in which such recipients are likely to be located (1.4(g)), unless it is unreasonable or impracticable to do so. This includes a likely disclosure to a related body corporate that is located overseas.

i An example of when it would be impracticable to list all countries to which the information is likely to be disclosed is where personal information is to be disclosed to numerous overseas recipients and the burden or determining where those recipients are likely to be located would be excessively time consuming, costly, or inconvenient in all the circumstances. However, an APP entity will not be excused from doing so on the basis that it would be inconvenient, time-consuming or impose a cost to do so.

2.4.3 The Office of the Australian Information Commission has also published guidelines containing some non-mandatory but suggested content for inclusion in an entity's Privacy Policy, such as requiring an individual to follow a procedure when requesting the access and correction of personal information.

3 EXTERNAL SYSTEMS

3.1 Website

3.1.1 A Company's website should display the Company's most up-to-date Privacy Policy at all times. While this is not a statutory requirement to specifically do so, it is the most convenient way to discharge the Company's duty under APP 1.5 and 1.6 to take steps to make its Privacy Policy available free of charge.

3.1.2 It should also adhere to the APPs in respect of the personal information in displays on its website.

3.2 Third Party Outsourcing

3.2.1 Third party outsourcing will require the disclosure of information. Companies should mainly consider three aspects of Privacy Law when outsourcing:

a Firstly, whether they hold personal information about individuals;

b Secondly, whether part of the outsourcing will involve the disclosure of that personal information to third parties; and

c Thirdly, the statutory requirements surrounding the disclosure of that personal information. The statutory requirements differ for cross-border disclosure, and disclosure within Australia. The Company must therefore consider the location of each third party.

3.2.2 *Cross-Border Disclosure of Personal Information*

a When a Company is outsourcing its services and disclosing personal information as part of that process to a third party who is located overseas, the Company must comply with the requirements of disclosure of information contained within APP 8.

b APP 8 states that, before the entity discloses personal information about an individual to an overseas recipient, the entity must "*take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles ... in relation to the information*"[1]. To comply with this, you would need to obtain appropriate undertakings from the third party to comply with the APPs. Depending on the third party, this may not be possible.

c Subclause 8.2 provides some main exceptions to this responsibility, including:

i Where the entity reasonably believes that the overseas recipient is subject to a law that has the effect of protecting the information in a way that is similar to the protection that the information would receive under the APPs AND there are mechanisms available that the individual can utilize to enforce the protection of that law or authority; or

[1] *Privacy Act 1988* (Cth) Schedule 1 clause 8.1.

ii Where the entity expressly informs the individual that if they consent to the disclosure of the information to an overseas recipient, the information will not be required to be protected by the responsibility stated above AND the individual consents to this disclosure; or

iii The disclosure of the information is required or authorized by or under Australian law.

d Companies should also be aware that where they are simply storing personal information on a cloud computing system that is located overseas, this can be considered to be cross-border disclosure. Cloud computing will be discussed later in this paper.

3.2.3 *Domestic disclosure*

a The disclosure of personal information to third parties located within Australia will follow the rules described in APP 6: Use or disclosure of personal information.

b "Disclose" is not defined in the Act and takes its ordinary meaning. Disclosure will occur where the information is made known outside of the holding entity.

c An entity can only use and disclose personal information for the primary purpose for which is was collected. It can be used for a purpose other than the primary purpose in limited circumstances, including where an individual has consented to such use or disclosure, or the individual would reasonably expect the disclosure to occur, and the secondary purpose is related to the primary purpose of collection (or directly related in the case of sensitive information).

d Therefore, if an entity is outsourcing some of its functions to a third party in the course of conducting its business activities, and that outsourcing involves the disclosure of personal information to that third party, the entity will be in compliance with APP 6. This is because they will have disclosed the information for the primary purpose for which it was collected, that is, providing services to the client. The entity should obtain contractual undertakings from the third party to comply with its Privacy Policy and the APPs, to ensure that there is no breach of the individual's privacy by the third party.

e An important exception to note about this APP is that it does not apply to the disclosure of personal information for the direct marketing of the entity.

3.2.4 If the APPs for cross-border and domestic disclosure apply, the Company will need to ensure that they have complied with them, or have methods in place to ensure compliance, *prior* to the disclosure of this information. We suggest that you seek legal assistance to do so.

4 SWAPPING DATA

4.1 Swapping data addresses two aspects of privacy law:

4.1.1 The outgoing data is subject to the rules of the use and disclosure of personal information; and

4.1.2 The incoming data is subject to the rules of the collection of personal information.

4.2 For the purpose of this section, we will consider “data” to be personal or sensitive information.

4.3 *Outgoing data*

4.3.1 The outgoing data will be subject to the same principles as outlined above in “third party outsourcing”. Again, the Company will have to be aware of the location of the entity to whom they are disclosing the data, and the specific rules surrounding that disclosure.

4.4 *Incoming data*

4.4.1 We have briefly discussed the principles surrounding the collection of incoming data in respect of CCTV surveillance. However, the collection of data from a third party source should be carefully considered.

4.4.2 We have outlined above that an APP entity may not collect personal information unless the information is reasonably necessary for one or more of the entity’s functions or activities.

4.4.3 This may raise significant concerns. It is important that the organisation is able to justify the collection of all of the personal information, and provide a valid reason for the collection of that information as being necessary to facilitate one of its functions or activities.

4.4.4 A situation where it may not be “reasonably necessary” for the entity to collect personal information is where it requires only a portion of the information that it collects. For example, if it only required the individual’s name, however also acquires the individual’s residential address and telephone number in the process of the data swap, by way of the disclosing entity disclosing the entire file of information that they have obtained about the individual.

a If the entity has only requested certain information as part of the data swap, however was provided with additional information, the additional information will then be considered to be “unsolicited personal information” and subject to the rules of APP 4.

b APP 4 requires that, upon receipt of that information, the entity considers and determines whether they could have collected the information if they had solicited it under APP 3. If so, they may keep the information and treat it in accordance with the APPs as if it had been solicited. If it could not have, they must destroy or de-identify the information.

4.4.5 APP 3.5 and 3.6 state how the information must be collected. This has also been outlined above. It must be by lawful and fair means, and collected directly from the individual unless an exception applies.

a When swapping data, an entity will not be collecting the information directly from an individual. The entity must therefore be able to rely upon an exception to be able to lawfully collect that information.

i Under APP 3.6(b), an Employer must assess the collection of each piece of information on a case-by-case basis and determine whether it is unreasonable or impracticable for the entity to collect it directly from the individual.

ii If the entity is collecting personal information from a third party which it could easily obtain from the individual, it is likely that the entity will be in breach of the APPs. The fact that it is more convenient for the entity to gather the personal information through a data swapping mechanism from a third party, rather from the individual, is not a defence to a breach of this obligation. The Act exists to protect the individual's rights to privacy of their personal information, and a mechanism to achieve this is to require as far as possible that the information be consensually supplied by the individual themselves.

4.4.6 APP 5 requires that if an entity is collecting personal information, it must inform the individual concerned of the entity's collection of the individual's personal information before or, if that is not practicable, as soon as practicable after, it collects the information. It must take reasonable steps to inform the individual of the matters referred to in APP 5.2. These include:

a The entity's contact details (5.2(a));

b The fact that they have collected, or will collect, the information, and the circumstances of collection (such as date, time, method, place (5.2(b));

c Whether the collection is required or authorised by law (5.2 (c));

d The purpose of collection (5.2(d)). This complements APP 3 – that the collection must be reasonably necessary for the functions or activities of the entity;

e The consequences if the information is not collected (5.2(e));

f The entity's usual disclosures of information (5.2(f));

g Information about the entity's Privacy Policy, and that it contains information about how the individual may access the personal information about the individual that is held by the entity (5.2(g)-(h)); and

h Whether the entity is likely to disclose the information to overseas recipients and the countries in which they are location (5.2(i)-(j)).

To ensure that they have taken "reasonable steps" as required by the legislation, an entity should develop procedures that are uniformly applied prior to collecting the information, This could take the form of requiring that a standard collection notice for notifying individuals regarding the collection of personal information is sent out with the forms, or included in the body of the forms, that clients must complete (if the Company uses these methods to obtain information). If an individual is providing information via an online form, an entity could require the individual to confirm that they have read the collection notice before the individual is able to provide their personal information.

5 DATA TRANSFER AND IMPACT OF CLOUD COMPUTING: COMPLIANCE OF OUTSOURCING

5.1 *Data transfer*

5.1.1 The transfer of data is subject to the same rules of disclosure as outlined in “outgoing data” above and “third party outsourcing”.

5.2 *Cloud Computing*

5.2.1 There has been a recent shift to cloud computing, that is, the virtual storage of information by a storage provider. Often these providors are located overseas, resulting in the disclosure of personal information over international borders.

5.2.2 Therefore, the disclosure of information to these third party storage providors is subject to APP 8, the cross-border disclosure of personal information, which has been discussed extensively above in relation to data swapping with other entities. A summary of this APP is that if an entity uses cloud computing located overseas, they must take reasonable steps to ensure that the overseas providor does not breach the APPs.

5.2.3 APP 1 also requires that an entity states in their privacy policy the overseas countries to which such recipients are likely to be located if it is practicable to specify those countries in the policy. In this particular instance, it may not be practicable to specify this in the policy. As each cloud server is generally located across multiple countries, it will be extremely onerous, if not impossible, to ascertain on which cloud server in which country an individual’s personal information will be located at different times.

6 QUESTIONS?