SOURCING REFERENCE GUIDE

A reference tool for customers and service providers explaining current best practice and thinking from our global team.

1. OUTSOURCING AND THE NEW AUSTRALIAN PRIVACY LAW[1]

By Alec Christie, Partner, and Rose Bollard, Graduate, DLA Piper Sydney

IN A NUTSHELL

In Australia all APP Entities which collect, use or disclose Personal Information must, under the *Privacy Act 1988* (Cth) (**"Act"**), take reasonable steps to protect the information from misuse, interference, loss, unauthorised access, modification and disclosure. If an APP Entity discloses or outsources the handling of Personal Information to another APP Entity (ie a Service Provider in Australia) there is no specific requirement for the disclosing APP Entity to ensure that the Service Provider complies with Australian privacy law because the Service Provider is already subject to Australian privacy law. However, the disclosing APP Entity's obligations to protect the information will extend to carrying out some due diligence to ensure that it selects a Service Provider (even one in Australia) which has compliant privacy practices and processes.

If an APP Entity discloses Personal Information to a foreign Service Provider (ie an Overseas Recipient) it must take reasonable steps to ensure that the Overseas Recipient will not breach the APPs in relation to the information disclosed and the disclosing APP Entity will remain responsible for ensuring that the Overseas Recipient handles the information in accordance with Australian privacy laws, unless the APP Entity obtains the informed consent of the relevant individuals to their information being disclosed to the Overseas Recipients. However, the disclosing APP Entity is not required to take these steps if the Overseas Recipient is subject to privacy laws and access to a complaints/determination system which are similar to those in Australia (or another of the limited exceptions applies). In practice, currently, this would be limited to disclosure to a recipient in the EU.

[1] The Australian version of Chapter 12 of DLA Piper's *"Sourcing Reference Guide"*.

Figure 1: Glossary of Terms

Australian Privacy Principles or **APPs**: are the set of privacy principles contained in the *Privacy Act 1988* (Cth) which apply to private organisations and Australian Federal, ACT and Norfolk Island Government agencies from 12 March 2014, replacing the National Privacy Principles for private organisations and the Information Privacy Principles for Government agencies.

APP Entity: is any Government agency or private organisation subject to the APPs (ie any Australian entity or other entity carrying on a business in Australia). An "organisation" includes an individual, body corporate, partnership, any other unincorporated association or a trust which is not a small business operator (ie operator of a business with a turnover of less than AU$3 000 000 that does not deal in Personal Information or collect/use health information as part of a health service), registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory. In European terms, an APP Entity may be a "data controller" or a "data processor".

Disclosure: means both the disclosure and transfer of information. That is, it includes both providing access to information held in Australia to an entity located outside of Australia as well as actual transfer of the information outside of Australia to an Overseas Recipient.

Overseas Recipient: means a person or organisation to whom an APP Entity discloses Personal Information and which is not in Australia. In European terms, the Overseas Recipient is most likely a "data processor".

Personal Information: is information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion. For example, a person's name, bank account number, address, registration number, Tax File Number, email address, job title, location and IP address can all constitute personal information.

Sensitive Information: is a type of Personal Information which is about or includes information on an individual's race or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, trade union membership, physical or mental health, sexual preference or practices, criminal record or involvement in criminal proceedings. It also includes an individual's health information, genetic information that is not otherwise health information, biometric information that is to be used for the purpose of automated biometric verification or biometric identification and biometric templates.

Service Provider: means an organisation which provides services (whether under an outsourcing arrangement or otherwise) to an APP Entity that require the handling of personal information. A Service Provider in European terms may be a "data processor".

PROCESS FOR ON-SHORE AND OFF-SHORE OUTSOURCING

If an APP Entity outsources services which require the Service Provider to handle Personal Information (including Sensitive Information), the APP Entity should take certain steps to ensure that there are adequate protections in place to protect the Personal Information. If the Service Provider is overseas (ie an Overseas Recipient), the APPs impose additional requirements on the APP Entity before it can disclose the information to the Service Provider.

GENERAL OUTSOURCING REQUIREMENTS (WHETHER TO AN ON-SHORE OR OFF-SHORE SERVICE PROVIDER)

1) Ensure that the disclosure of Personal Information to a Service Provider complies with the Australian Privacy Principles

The APPs impose a number of restrictions on how Personal Information (and Sensitive Information) can be collected, used and disclosed and so, before disclosing information to a Service Provider, an APP Entity should ensure that the disclosure is compliant with the APPs. The two key APP requirements are as follows:

- For Personal Information the APP Entity must notify individuals of (and for Sensitive Information obtain consent for) the purposes for which their information is collected, held, used and disclosed. Therefore, the APP Entity's privacy policy should state that the Personal Information is disclosed to Service Providers in an outsourcing arrangement ("data processing") and state the broad category of services those companies will provide. Individuals need to be notified of (or consent to, for Sensitive Information) the privacy policy before or at the time of the collection of their Personal Information (or as soon as possible afterwards if neither option is practical). There are no exceptions to the notification/consent requirement.
- APP Entities can only use Personal Information for the primary purpose of its collection or a secondary purpose if it has the individual's consent or if the secondary purpose is related to the primary purpose (or directly related to the primary purpose consented to, if it is Sensitive Information). Therefore, if the Personal Information was not collected for the primary purpose of the activities to be performed by the Service Provider or those activities are not related to the original purpose for which the information was collected, the APP Entity cannot disclose the information to the Service Provider without the individual's consent.
  - For example, if an Australian online shop collects Personal Information for processing payments but the payments are processed by a third party company, the online shop would not need consent for the disclosure of the information to the third party as processing payments is a primary reason for which the information is collected (assuming the privacy policy includes this purpose and the fact of a disclosure to a third party to do this).

2) Assess the type of Personal Information and appropriate level of security required to protect it

APP Entities considering disclosing Personal Information to a Service Provider (or any other organisation) should confirm a level of security for Personal Information exists that is appropriate both to the harm that might result from the unauthorised use or disclosure of the Personal Information and to the nature of the Personal Information to be protected. For example:

- If Sensitive Information is being disclosed the security measures that the Service Provider receiving the information has in place will generally be required to be at a higher level than if only handling Personal Information (eg names and email addresses).
- Financial information such as bank account numbers and credit cards details, although not categorised as "sensitive personal data" under the Act, has the potential to result in much harm if wrongfully disclosed and therefore entities handling this information are advised to implement the highest level of security in relation to this information.

3) Consider means of providing adequate security of data

Where an APP Entity discloses Personal Information to a Service Provider, the APP Entity **should**:

- choose a Service Provider that can provide sufficient guarantees in respect of security measures;
- take reasonable steps to ensure (eg audit) that the Service Provider complies with those measures; and
- ensure that the handling of the Personal Information is carried out according to the terms of a written agreement.

4) Conduct due diligence on the Service Provider to ensure adequate level of protection and security

The obligation to choose a suitable Service Provider with reliable staff indicates the need to carry out some due diligence of the Service Provider prior to transferring any Personal Information or entering into any formal agreement. This will be true regardless of where the Service Provider is located.

5) Consider if you need undertakings from third parties

It is prudent to confirm (as best practice) that the Service Provider takes reasonable steps to ensure that any employees responsible for handling Personal Information are reliable. This would include the need to obtain confidentiality undertakings from employees/third parties as appropriate to their role in Personal Information handling.

6) Enter into a formal agreement

It is important to note that the *Privacy Act* does *not* impose an express legal or statutory obligation directly upon an APP Entity to ensure that Australian Service Providers comply with the APPs. However, as part of the APP Entity's obligation to protect the Personal Information, it is best practice to have in place robust contractual provisions to restrict and control the usage and storage of Personal Information being processed on its behalf (often requiring the Australian Service Provider to comply with the APP Entity's privacy policy and directions). Most of the requirements set out above can be stipulated as contractual obligations imposed on the Service Provider.

ADDITIONAL OFF-SHORE OUTSOURCING REQUIREMENTS

In order to disclose Personal Information outside of Australia, APP 9 requires organisations to take "reasonable steps" to ensure an overseas recipient does not breach the APPs in relation to the information. The most simple means of doing so, in practice, is for the APP Entity to enter a contractual arrangement with the Overseas Recipient, requiring it to handle information in accordance with the APPs and building in audit rights etc. What actions constitute "reasonable steps" will depend on the circumstances, including the nature of the Personal Information, the APP Entity's relationship with the overseas recipient, the risk of harm to the individual if the information is mishandled and the practicality of taking particular steps. However, the disclosing APP Entity will remain liable for any breaches of the APPs by the Overseas Recipient. That is, breaches of the APPs by an Overseas Recipient will be deemed to be those of the disclosing APP Entity and to have occurred in Australia.

There are several exceptions to the requirement to take "reasonable steps". The APP Entity may disclose Personal Information to an overseas recipient if the individual provides informed consent to the disclosure after being expressly informed of the consequences of his/her consent and that the APP Entity will not ensure that the overseas recipient will comply with the APPs. There is also an exception if an APP Entity reasonably believes that the recipient of the information is subject to a law or binding scheme that has the effect of protecting the information in a way that is at least substantially similar to the way in which the APPs protect the information and with access to a similar complaints/determination system. Also, if the disclosure is required or authorised by the law, the APP Entity does not need to take these "reasonable steps".

KEY ISSUES

THE THIRTEEN AUSTRALIAN PRIVACY PRINCIPLES

The *Privacy Act 1988* (Cth), contains thirteen principles with which all APP Entities are required to comply (*see Figure 2 "The Australian Privacy Principles"*).

Figure 2: Overview of the Australian Privacy Principles:

1. APP Entities must manage information in an open and transparent way which includes having an up-to-date privacy policy.
2. APP Entities must provide individuals with the option of not identifying themselves or of using a pseudonym when dealing with the APP Entity.
3. Personal Information can only be collected if it is reasonably necessary for, or directly related to its activities or functions. Consent is required for the collection of Sensitive Information.
4. An APP Entity must destroy or de-identify unsolicited Personal Information unless the APP Entity could have collected the information itself or it is contained in a Commonwealth record.
5. An APP Entity which collects Personal Information about a person must notify the person of a number of matters or otherwise ensure that they are aware of them.
6. If an APP Entity collects Personal Information for a primary purpose, it cannot use or disclose the information for another purpose unless it has the individual's consent or an exception applies.
7. An APP Entity cannot use or disclose Personal Information for the purpose of direct marketing unless the person would have expected it to be used for that purpose or they provided their consent. The exceptions do not apply to Sensitive Information.
8. An APP Entity must take reasonable steps to ensure an Overseas Recipient does not breach the APPs before disclosing Personal Information to it unless an exception applies (eg consent).
9. An APP Entity must not use a government related identifier of an individual as its own identifier of the individual.
10. An APP Entity must ensure that the Personal Information it collects is accurate, up-to-date and complete.
11. An APP Entity must take reasonable steps to protect Personal Information it holds from misuse, interference, loss, unauthorised access, modification or disclosure.
12. An APP Entity has certain obligations when an individual requests to be given access to Personal Information held about them by the entity.
13. An APP Entity has certain obligations in relation to correcting the Personal Information it holds about individuals.

"COLLECTION" OF THE PERSONAL INFORMATION BY THE SERVICE PROVIDERS

As soon as an Australian based Service Provider (or any Service Provider obliged to comply with the APPs) receives or accesses Personal Information originally collected by an APP Entity, independent privacy obligations of that Service Provider are triggered in respect of that Personal Information which is considered to also have been "collected" by the Service Provider. The main obligation for "collection" is contained in APP 5 which requires that persons whose information is collected or accessed are notified of a number of mandatory matters including the contact details of the relevant entity, how the information will be handled and how it can be corrected. There are no exceptions to this obligation. That is, there is no distinction in Australian privacy law/privacy obligations, as in the EU, between a "data controller" and "data processor".

In addition, the Service Provider can only use the information for the purpose for which it was originally collected (unless an exception applies). For example, if the information was originally collected for the purpose

of processing payments for an online store, the Service Provider cannot use the personal details for market research.

This notification requirement on "collection" by the Service Provider may be quite onerous in practice. One solution may be for the company (ie the APP Entity) which originally collects the information to provide a link to the Service Provider's (or Service Providers') privacy policy when notifying the individual of its own privacy policy and to obtain any necessary consents for the collection and use of Sensitive Information.

MANAGING DATA PROTECTION THROUGHOUT THE LIFE OF THE CONTRACT

As explained above, an APP Entity's responsibility to protect Personal Information from interference extends to assessing whether a Service Provider has good privacy practices before engaging it to provide services which require it to handle Personal Information. Furthermore, this naturally extends to ensuring that the Service Provider has adequate practices throughout the lifetime of the contract and that the Service Provider continues to handle the information in an appropriate manner. The APP Entity must put into place systems that allow it to regularly review or "audit" the Service Provider's data handling procedures.

CONCLUSION

If an outsourcing arrangement includes the disclosure of Personal Information to a Service Provider, then the contract between the parties should contain a privacy clause and comprehensive information handling instructions. The clause should, at a minimum:

- stipulate that the Service Provider will only use the Personal Information on behalf of the APP Entity and only in accordance with the APPs and the APP Entity's instructions;
- require the Service Provider to implement and maintain appropriate technical and organisational measures to prevent against the unlawful use or disclosure of Personal Information in consideration of the type of Personal Information being processed;
- require the Service Provider not to do anything that would result in the APP Entity being in breach of the Privacy Act/APPs;
- oblige the Service Provider to return or delete and/or destroy the Personal Information (at the APP Entity's option) at the earlier of the end of the term of the agreement or termination;
- require the Service Provider to notify the APP Entity in the event of any claim, data loss or other complaint received which relates to the processing of Personal Information; and
- include an indemnity protecting the APP Entity sending the information for any losses or liability arising from the Service Provider's breach of the clause, and data loss and instructions (including providing all assistance necessary).

If the outsourcing arrangement includes off-shoring Personal Information, the APP Entity must take reasonable steps to ensure that the Service Provider will not breach the APPs in relation to the information or that an exception applies (such as obtaining consent or ensuring the Service Provider is subject to a similar privacy law and complaint/access system).

SECTOR/SERVICE SPECIFICS

In addition to the above, it is important to remember that compliance with the Privacy Act is not the end of the story. Where APP Entities are regulated by other bodies (eg financial services sector), additional regulations, sanctions and obligations such as mandatory breach notification requirements might impact upon the obligations set out in the agreement and the level of data security due diligence needed before an agreement is finalised.

LOCAL LAWS

In addition, some countries have laws that stipulate specific IT security requirements of which APP Entities should be aware. In the U.S., for example, data security legislation has been prioritised above data privacy laws and twenty-three states have passed data breach notification laws. These statutes require companies to notify customers if there is reason to believe that unencrypted customer data has been accessed by an unauthorised person. This obligation goes beyond the requirements of the current Australian law.