Corporate

February 2014

www.landers.com.au

Privacy Reforms

Time is running out to comply

Summary

From 12 March 2014, there will be significant changes to the current privacy laws in Australia. In August 2013 we discussed these changes including a new unified set of 13 'Australian Privacy Principles' (**APPs**) which will regulate the handling of personal information.

The APPs will replace the current National Privacy Principles (**NPPs**), which apply to the private sector, and the Information Privacy Principles (**IPPs**), which apply to the federal public sector. These changes are now imminent and will have a significant impact on the way affected entities in the private sector and the federal public sector (**APP entities**) handle personal information. If you are unsure about whether your organisation is an APP entity, please seek legal advice.

Importantly, the reforms will also introduce civil penalties for certain breaches. Penalties of up to $1.7 million can apply to body corporates and $340,000 to non-body corporates, (including individuals), for serious or repeated interferences with the privacy of an individual[1].

Organisations will now be required to maintain a detailed privacy policy which governs their collection and handling of personal information and to provide a collection notice and access to the privacy policy when collecting personal information from individuals. In this eBulletin, we discuss these two key documents, as well as looking at the new accountability regime for organisations which send personal information overseas.

A proactive approach to privacy

Under the revised Privacy Act, organisations must take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs (APP1.2). Organisations will need to be proactive and to consider, for example:

- carrying out regular staff training on compliance with the APPs;
- implementing procedures for identifying and managing privacy risks; and
- ensuring that security systems are in place for the protection of personal information.

Developing and maintaining a robust and up-to-date privacy policy and collection notices will also assist organisations to meet this obligation.

Privacy policies

Organisations are required to have a clearly expressed and up to date privacy policy dealing with how they manage personal information (APP1.3). Organisations in the private sector are currently required to maintain a privacy policy, however the new laws will introduce prescribed minimum content for those policies (APP 1.4). As the IPPs do not require agencies to have a privacy policy, this will be a new requirement for organisations in the federal public sector.

The following checklist may assist you in complying with the new requirements for your organisation's privacy policy.

Privacy policy requirements	
☑	Does your organisation have a privacy policy?
☑	Does your organisation's privacy policy contain the following information: • The kinds of personal information that the organisation collects and holds? • How the organisation collects and holds personal information? • The purposes for which the organisation collects, holds, uses and discloses personal information? • How an individual may access his/her personal information held by the organisation and seek correction of such information if necessary? • How an individual may complain about a breach of the APPs and how the organisation will deal with such a complaint? • Whether the organisation is likely to disclose personal information to overseas recipients and, if so, the countries in which such overseas recipients are likely to be located?
☑	Is the organisation's privacy policy clearly expressed?
☑	Are there systems in place to ensure that the organisation's privacy policy is updated regularly?
☑	Has the organisation taken reasonable steps to make its privacy policy available free of charge (for example on its website)?
☑	Does the organisation have practices or procedures in place to ensure reasonable steps are taken to give a copy of the policy to a person or entity that requests it in a particular form?

Collection notices

Organisations will also be required to notify individuals (or make them aware) of certain specific matters when collecting their personal information (APP5.1). Organisations must do this either before, at the time of or as soon as practicable after the collection is made.

These prescribed matters are set out in APP5.2. They are far more extensive than the current notification requirements for the federal public sector under the IPPs.

For organisations in the private sector, a significant new prescribed matter is whether the organisation is likely to disclose the personal information to an overseas recipient and, if so, where those recipients are likely to be located. For example, many organisations are now storing or backing-up their data in "the cloud". Where the cloud service provider is based outside Australia, organisations should consider whether this constitutes disclosure of personal information to an overseas recipient under the legislation.

Organisations will often be able meet their notification obligations by providing individuals with a collection notice (ie, a document setting out the prescribed matters). The following checklist may assist you in drafting new, or reviewing existing, collection notices in compliance with the prescribed minimum content requirements.

Collection notice content requirements	
☑	The identity and contact details of the organisation.
☑	The fact and circumstances of collection if the information is collected from someone other than the individual (otherwise the individual may not be aware that the organisation has collected the personal information).
☑	Whether the collection is required or authorised by law.
☑	The purposes of collection.
☑	The main consequences for the individual if the personal information is not collected.
☑	Any other organisation or person to which the organisation usually discloses personal information of the kind collected.

☑	That the organisation's privacy policy contains information about: • seeking access to, and correction of, the personal information; and • making privacy complaints and how they are handled.
☑	Whether the organisation is likely to disclose personal information to overseas recipients and, if practicable, the countries where they likely to be located.

Disclosing personal information overseas

Before an organisation discloses personal information overseas, it must take reasonable steps to ensure that the recipient of the personal information does not breach the APPs (APP8.1).

There are several exceptions to APP8.1. For instance, APP8.1 does not apply where the APP entity reasonably believes that the overseas recipient is protected by a similar law or binding scheme in their own country and that there are mechanisms that the individual can take to enforce that protection (APP8.2(a)) or the individual consents to the disclosure after being expressly informed of the disclosure and the effect of his/her consent (APP8.2(b)).

Importantly, where APP 8.1 applies, an act done by the overseas recipient is now considered to have been done by the APP entity itself, therefore in this situation, the APP entity would be in breach of the APPs.

Given the international scale of modern communications networks and the widespread use of internet-based data services, data of all kinds is regularly sent to overseas recipients by organisations. In most cases the provision of information to an overseas service provider (including a related company) will be a disclosure within the meaning of APP8.

In some limited circumstances, sending information to a third party overseas to be merely stored or processed on behalf of the organisation (such as certain types of 'cloud' services) will not of itself be considered a disclosure of the information (this depends on the degree of control retained by the organisation and the services being provided by the third party).

Where there is a disclosure of personal information overseas, the organisation will be liable unless it had reviewed the circumstances in which the information was disclosed and taken appropriate action.

Organisations may seek to minimise the risk of liability by including appropriate provisions in their contract with the overseas recipient. For example, they might impose express obligations on the recipient to comply with the APPs, including an indemnity for claims against the organisation arising from a breach by the recipient of the APPs.

Requirements when sending personal information offshore	
When disclosing personal information to a recipient overseas, an organisation must:	
☑	(a) form a reasonable belief that the information is subject to a law or binding scheme in the overseas jurisdiction which will adequately protect the personal information; OR
☑	(b) obtain the individual's informed consent to the overseas disclosure; OR
☑	(c) take reasonable steps to ensure the overseas recipient does not breach the APPs.

What to do next…

The changes to the Privacy Act will come into effect next month, and organisations should already be identifying and reviewing their existing compliance activities in relation to the handling of personal information. It is important to ensure your organisation meets and complies with these new requirements. This includes reviewing and updating existing privacy policies and collection notices.

The national privacy regulator, the Office of the Australian Information Commissioner, has published draft guidelines on how it will interpret and apply the APPs when exercising its functions and powers under the Privacy Act. Public consultation has now closed and final versions are due to be published in February 2014 which will assist you in achieving compliance with the Privacy Act changes.

If you would like Lander & Rogers to assist or advise your business in preparing for the Privacy Act changes, please contact us.

Author

Jessie Bridge

1 *Breach of an APP is defined to be an interference with the privacy of an individual.*

Further information

Natalie Cambrell | Partner
+61 3 9269 9583
ncambrell@landers.com.au

Robert Neely | Partner
+61 2 8020 7704
rneely@landers.com.au

Richard Redman | Senior Associate
+61 3 9269 9664
rredman@landers.com.au

Luong Truong | Lawyer
+61 3 9269 9529
ltruong@landers.com.au