Executive Summary

Privacy Awareness Week for 2013 commences on 28 April 2013 and this year’s focus is privacy law reform. With Australia’s privacy law regime being overhauled recently when the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) became law in December 2012, now is the perfect time to familiarise yourself with the new requirements and ensure that your company fully complies with those requirements.

There are a number of significant changes, including the introduction of mandatory privacy principles which will affect the way your company collects, uses, discloses, transfers across borders and stores personal information. One of the key steps which needs to be taken is to ensure that your company’s Privacy Policy complies with the new requirements.

To ensure that companies take their privacy obligations seriously, the Privacy Commissioner can now seek substantial penalties for non-compliance, with maximum penalties of $340,000 for individuals and $1.7 million for companies.

Have we got your attention? Read on to find out more.

Australian Privacy Principles

The Privacy Amendment (Enhancing Privacy Protection) Act 2012 (the Act) introduces the Australian Privacy Principles (APPs). The APPs combine and replace the National Privacy Principles and the Information Privacy Principles contained in the Privacy Act 1988 (Cth). The APPs set out obligations with which APP entities (being an “organisation” or an Australian Government agency) must comply relating to the collection, storage, security, use, disclosure, access and correction of personal information acquired by an entity. Broadly speaking, personal information is any information which can identify a person.

These obligations apply generally to companies with a turnover in excess of $3 million; however, in certain circumstances, they will apply to companies with an annual turnover of less than $3 million. In any event, all companies should consider complying with the APPs, if not already, because of the strong message to consumers that the company, regardless of its size, recognises the importance of treating personal information in an appropriate and secure manner.

Changes to Privacy Regulation

So how will the changes impact upon the way in which your company handles personal information?

Privacy Policies

Companies are required to implement practices and policies so that their management of personal information is open and transparent. In particular, your company must have a privacy policy which must include:

- details of the kind of personal information collected;
- how personal information is collected and held;
- the purposes of collection;
- how individuals can seek access to and/or correct personal information;
- how a complaint concerning privacy may be made; and
- whether the personal information will be disclosed to overseas recipients and, if so, the countries where the recipients are located (if practicable).
Accordingly, privacy policies need to be updated to meet the new requirements. For example, it was previously sufficient for a privacy policy to state that a company “collects personal information from its customers for the purpose of providing services to those customers”. It is now necessary for the privacy policy to stipulate what kind of personal information is being collected and the purpose of collection. Moreover, multinational companies need to take special care to meet the new obligations and this is particularly relevant for all companies operating in Australia that are part of a global group.

Notification of Collection
Companies were required previously to notify an individual before or at the time they collected the individual’s personal information (or as soon as practicable after). However, if companies now collect an individual’s personal information from someone other than the individual, the company must take reasonable steps to notify the individual or ensure that they are aware that the company has collected the information and the circumstances in which the information was collected. These matters should be addressed in your company’s Privacy Policy, if relevant.

Direct Marketing
The use of personal information in the promotion and sale of goods and services directly to new and existing customers will now be more heavily regulated. If you hold personal information about an individual, you must not use or disclose the information for the purpose of direct marketing. However, there are various exceptions. You will be permitted to use personal information for direct marketing if:

- your business collected the information from the individual;
- the individual would reasonably expect your business to use or disclose the information for the purpose of direct marketing;
- you provide a simple means for the individual to request to opt-out from receiving direct marketing communications; and
- the individual has not requested to opt out.

If the individual would not reasonably expect their personal information to be used or disclosed for direct marketing or your company has obtained the personal information from a third party, your company can only use the personal information for direct marketing if:

- the individual consented to the use or disclosure for this purpose or it is impracticable to obtain their consent;
- you provide a simple means for opting out of direct marketing and the individual has not opted out; and
- your company includes a prominent statement in each direct marketing communication it sends stating that individuals can request to stop receiving direct marketing and no request has been made.

However, companies should also be mindful of their obligations under the Spam Act 2003 and the Do Not Call Register Act 2006. In some circumstances, even if the company complies with APP 7, sending such a marketing message may still breach these Acts.

Individuals will also now have the right to ask your company to confirm how their personal information came into your company’s possession. Your company is required to provide the source, unless impracticable or unreasonable, within a reasonable time and at no cost to the individual.

Companies are also able to use sensitive information (i.e. health information, genetic information, political opinions, and information about racial or ethnic origins) for direct marketing purposes if the individual consented to the use or disclosure for that purpose.

Care will need to be taken by companies to ensure that any marketing complies with this principle. It is particularly important in respect of online marketing targeting Australians which is often conducted from outside Australia.

Cross-border Disclosures of Personal Information
Before providing an overseas organisation (including a related body corporate) with personal information about an individual, APP 8.1 requires that an Australian organisation must take reasonable steps to ensure that the overseas recipient does not breach the APPs. In some circumstances, Australian organisations will remain accountable for information sent overseas and will be liable for breaches of the APPs by overseas recipients. This is a significant change to Australia’s privacy regime and will impact upon Australian subsidiaries of overseas companies.

APP 8.1 provides a number of exceptions, and states that reasonable steps will not be required, for example:

- if the recipient is subject to a law which protects the personal information in a way which is similar to the protection provided by the APPs; and
- there are mechanisms the individual can use in the overseas jurisdiction to enforce the laws. Companies will need to conduct inquiries in this regard.

Accordingly, adequate precautions must be in place to prevent unintended and unauthorised breaches of the APPs, particularly in a global context.

Access and Complaints
You must ensure that an individual is aware of:

- the fact that they can access their information;
- their rights of complaint and how they may complain;
- the purposes for which their information is collected; and
• any organisations to which the information may be disclosed, including overseas recipients. Examples may include third party vendors providing order fulfilment and other administrative services such as the preparation of mail-outs and credit card processing. ¹⁰

This information will need to be set out specifically.

Unsolicited Information

If your company deals with personal information which was not solicited by your organisation, the unsolicited information will also be regulated. Unsolicited information might be received from, for example, a member of the public sending a query to a company about its range of products.

When unsolicited information is received, you must, within a reasonable period, determine whether or not your company could have collected the information in accordance with the collection rules. The collection rules require that you only collect personal information that is reasonably necessary for, or directly related to, one or more of your organisation’s functions or activities. ¹² If so, the personal information is then regulated by the APPs in the same way as if it had been solicited.

However, where you receive unsolicited personal information which is not reasonably necessary for, or directly related to, one or more of your company’s functions or activities, the information must be destroyed or de-identified so that it is no longer personal information as soon as practicable (if lawful and reasonable to do so). ¹³

Undertakings and Civil Penalties

Greater powers will be held by the Australian Privacy Commissioner. Most notably, the Commissioner will be able to:

• obtain enforceable undertakings from an organisation; and

• apply to a court for a civil penalty order against organisations and individuals. Maximum penalties for serious or repeated interference with an individual’s privacy will be $340,000 for individuals and $1.7 million for companies.

Credit Reporting

In addition to the new APPs, the Act also makes significant changes to Australia’s credit reporting laws. We will prepare a separate Focus Paper outlining these new privacy-related credit reporting requirements.

How Might These Changes Impact on Your Business?

The changes to the Privacy Act will impact companies in various ways. We would strongly recommend that companies take the following steps:

• review and revise their privacy policy to comply with the mandatory requirements set out in the Privacy Act;

• when engaging in direct marketing, provide a clear and simple method that allows targeted consumers to opt out;

• keep more detailed, accurate and current records as to how personal information is obtained. (This would help ensure that the company is able to address queries from individuals who are able to request details of how their personal information was obtained by the company); and

• take steps to ensure appropriate measures are in place where personal information is likely to be sent overseas. (On the basis that your company may be liable for any breach, you should take steps to ensure that, if personal information is sent overseas, the recipient complies with stringent obligations in connection with the protection of privacy.)

What now?

• We would recommend that companies conduct a privacy audit to examine the extent to which the amendments to the Privacy Act will apply and the changes required to ensure compliance with the Privacy Act.

• Privacy training for relevant staff should be coordinated.

• You may also wish to appoint a Privacy Officer to deal with queries and compliance issues and maintain a specific email address for privacy queries.

• Adopting such measures will reduce your risk of breaching these requirements.

Conclusion

The amendments to the Privacy Act will impact upon the way in which your company collects, uses and discloses personal information. Your company will be expected to be fully compliant with the new obligations by 12 March 2014.

The arrival of Privacy Week is a timely reminder that you and your company should be considering and implementing the changes which you need to make to comply fully with the Privacy Act before the deadline.

Jamie Nettleton, Partner
Telephone +61 2 8915 1030
Email jamie.nettleton@addisonslawyers.com.au

Cate Sendall, Senior Associate
Telephone +61 2 8915 1028
Email cate.sendall@addisonslawyers.com.au
An “organisation” is an individual, body corporate, partnership or any other unincorporated association or trust, which is not a “small business” (a business with an annual turnover of less than $3 million) - s 6 Privacy Act 1988 (Cth).