SQUIRE SANDERS

NEW AUSTRALIAN PRIVACY PRINCIPLES: ARE YOU READY FOR MARCH 2014?

In November 2012 the Australian Parliament passed changes to the Australian Privacy Act 1988 (Cth). At the time, Squire Sanders provided an update to our clients about these new changes, and what would need to be done to make sure your business is compliant when the new changes come into effect (Amendments to the Australian Privacy Act, December 2012).

The biggest change to the Privacy Act 1988 (Cth) is the creation of new Australian Privacy Principles (APPs); a combination of the old Information Privacy Principles, for government, and National Privacy Principles, for business.

With only seven months to go until the new privacy principles come into effect, we have prepared the following summary of the new APPs so that you can make sure your business is ready for the changes when they come into effect. In particular, make sure you have a privacy policy in place as this goes from being a "nice to have" to a "must have".

The APPs apply to business organisations, such as companies and partnerships and to Australian Federal Government agencies (APP Entities). Small businesses (turnover less than AU$3 million) and certain other entities (such as registered political parties) are exempt from the legislation. If you are an APP Entity, you will need to comply with the following APPs.

APP 1 – Open and transparent management of personal information

This principle requires you to take reasonable steps to ensure that you comply with the APPs and can manage complaints or enquiries about your compliance with the APPs. This includes having a policy about the management of personal information by your organisation and making this policy available. The policy must include pieces of certain key information, which are listed in the principle.

APP 2 – Anonymity and pseudonymity

Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with you in relation to a particular matter, unless you are legally required or authorised to deal with people who have identified themselves, or it is impracticable for you to deal with people who have not identified themselves or who have used a pseudonym.

APP 3 – Collection of solicited personal information

APP 3 applies to the collection of personal and sensitive information solicited by you.

"Personal information" is information or an opinion about a person, when that person's identity can be linked to that information. You must only collect personal information by lawful and fair means.

"Sensitive information" is information that relates to a person's ethnic origin, sexual preference, religious, philosophical or political beliefs, criminal record, health information or genetic information.

APP 3 prescribes that you must not collect sensitive information about a person unless the person consents to the collection of the information.

APP 4 – Dealing with unsolicited personal information

If you receive unsolicited personal information, you must determine whether you could have lawfully solicited the information under APP 3. If you determine that you could not have collected the information, you must destroy the information (assuming it is lawful to do so). If you determine that you could have solicited the information under APP 3, then APPs 5 to 13 apply as though you had solicited the information.

APP 5 – Notification of the collection of personal information

If you collect personal information about a person, you must notify the person:

(a) of your name and contact details;

(b) that the information has been collected;

(c) what the information will be used for;

(d) to whom else the information will be disclosed;

(e) the rights of the person to access the information; and

(f) if you are likely to disclose the information to overseas recipients, in which countries the recipients of the information are likely to be located.

APP 6 – Use or disclosure of personal information

You must only disclose personal information about a person for the primary purpose for which it was collected unless the person consents to the disclosure or one of the exceptions applies. This principle does not apply to the use or disclosure by an organisation of personal information for the purpose of direct marketing or government related identifiers.

APP 7 – Direct marketing

You may only use personal information about a person for direct marketing if that person consents, or if the organisation collected the information from the person and the person would reasonably expect you to use or disclose the information for that purpose.

In any case, if you use personal information for direct marketing, you must provide a simple means by which the person may easily request not to receive direct marketing. You may not use personal information for direct marketing if a person has requested not to receive direct marketing or communications from you.

You may only use sensitive information about a person for direct marketing if the person has consented to the use of the information for that purpose. If you use a person's personal information for direct marketing, you must disclose the source of that information to the person if the person requests.

APP 8 – Cross-border disclosure of personal information

You must only disclose personal information about a person to an overseas recipient if:

(a) you inform the person that the overseas recipient will not be bound by the APPs and the person consents; or

(b) you have taken reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information; or

(c) you reasonably believe that the overseas recipient is subject to laws that protect the information in a substantially similar way to the APPs; or

(d) the disclosure is required by law; or

(e) it is to prevent a serious threat to the life, health or safety of a person or to public health or safety, or for certain government agency functions such as for diplomatic functions or in the course of war.

APP 9 – Adoption, use or disclosure of government related identifiers

A "government related identifier" of a person is an identifier that has been assigned by an agency, state or territory authority, or agent or contractor of a state or territory authority.

You must not adopt a government related identifier of a person as its own identifier unless required or authorised by an Australian law. You must not use or disclose a government related identifier of a person unless certain specific exemptions apply.

APP 10 – Quality of personal information

You must take reasonable steps to keep personal information that it collects up to date, accurate, complete and relevant.

APP 11 – Security of personal information

If you hold personal information you must take reasonable steps to keep it secure, and de-identify the information when it is no longer needed.

APP 12 – Access to, and correction of, personal information

If you hold personal information about a person, you must give the person access to that information upon request, unless an exemption applies. You must respond to the request for access within a reasonable period of time and must give access in the manner requested by the person, if reasonable.

Government agencies must not charge people for access to their personal information and if private organisations charge a fee, the fee must not be excessive. If you refuse to give a person access to their personal information, you must give the person a written notice setting out the reasons for the refusal and avenues of complaint about the refusal.

APP 13 – Correction of personal information

Upon request by a person you must take reasonable steps to correct personal information you hold about a person to ensure it is up to date, accurate, complete, relevant and not misleading.

If you have corrected personal information upon request of a person, and you have previously disclosed that information to another entity, upon request by the person you must take reasonable steps to notify the other entity of the correction.

If you refuse to correct personal information you hold when requested to do so by a person, you must issue the person with a notice setting out reasons for the refusal and avenues of complaint about the refusal. If you refuse to correct the personal information of a person, the person may require you to attach a statement to the personal information stating that it is deficient. If a person requests a correction of personal information or statement to be attached to personal information, you must respond within a reasonable period of time.

Alex Butterworth
Associate
T +61 2 8248 7809
E alex.butterworth@squiresanders.com

Richard Pascoe
Of Counsel
T +61 2 8248 7803
E richard.pascoe@squiresanders.com