# PRIVACY ACT GETS A REVAMP

The *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* was introduced to Parliament on 23 May 2012. The Bill amends the *Privacy Act 1988* (Act) and implements the Government's first stage response to the Australian Law Reform Commission's Report into Privacy. The majority of the new provisions have a deferred commencement of 9 months from the day the Bill receives the Royal Assent.

The Bill includes four main changes to the Privacy Act. These are:

- the creation of the Australian Privacy Principles, a single set of privacy principles which will apply to both Commonwealth agencies and private sector organisations (APP entities) and replace the current Information Privacy Principles and National Privacy Principles;
- more comprehensive credit reporting provisions and the expansion of the credit reporting system to include five new kinds of personal information;
- the introduction of new provisions on privacy codes and a new credit reporting code; and
- increased functions and powers for the Privacy Commissioner (Commissioner) including the extension of the Commissioner's audit powers to private sector organisations.

## Key Features of the new Australian Privacy Principles (APPs)

The new APPs replicate many of the concepts that currently exist in the Act. However, a range of amendments and additional protections have been included. Some of the key features of the new APPs are as follows:

- The terms "personal information" and "sensitive information" have been amended. The new definition of "personal information" refers to an individual who is "reasonably identifiable". Whether an individual is reasonably identifiable depends on the context and circumstances. If it is technically possible but not practically possible for an entity to identify an individual from information it holds, the individual will not be "reasonably identifiable". A consideration of the cost, difficulty, practicality and likelihood of linking information held by an entity with other information held by it must all be taken into account.

  The definition of "sensitive information" has been amended by adding references to biometric information and biometric templates. However, given the broad nature of what can be considered biometric information, the additional protections under the Act only extend to biometric information which is specifically being collected for the purpose of automated biometric verification or biometric identification.

- An obligation on entities to establish practices, procedures and systems to ensure compliance with the APPs including procedures to receive and respond to complaints and inquiries has been included in APP 1. In particular, an entity's privacy policy should be an "up-to-date", living document which is reviewed regularly. The Commissioner has new powers to initiate an investigation without a complaint into a possible breach of APP 1 including where an APP entity fails to have an up-to-date APP privacy policy.

- The list of items which must be included in an APP entity's privacy policy has been extended to include how the entity *holds* personal information, how an individual may complain about a breach of the APPs and how the entity will deal with such a complaint and, if an entity is likely to disclose personal information to overseas recipients, the entity must (if practicable) specify the countries in which such recipients are likely to be located.

- Individuals must have the option of dealing with an entity anonymously or through use of a pseudonym in relation to a matter. However, an entity will not be required to comply with this obligation where it is impracticable for the entity to deal with individuals who have not identified themselves.

- Direct marketing is now dealt with as a discrete principle. There is a general prohibition on organisations using personal information for direct marketing with a list of exceptions to the rule. One of these exceptions is that an organisation may use or disclose personal information (other than sensitive information) for direct marketing if: the organisation collected the information from the individual; the individual would reasonably expect the organisation to use the information for direct marketing; the organisation has provided a simple means by which the individual can request not to receive direct marketing; and the individual has not availed him or herself of this means. An opt-out rather than an opt-in requirement will be appropriate in circumstances where the individual itself has provided the information to the organisation. Where the organisation has obtained the personal information from someone other than the individual, if it is practicable for the organisation to obtain consent from the individual for the use of the personal information for direct marketing, the organisation must obtain such consent. The organisation must also provide a means for the individual to opt-out as well as comply with additional requirements to ensure the individual is aware of its rights and how to exercise its rights.
- A new principle is included for receipt by an entity of "unsolicited" personal information. An entity must destroy unsolicited information if the entity determines that it could not have collected the personal information in accordance with the "functions" test which applies to the collection of solicited personal information.
- A new accountability approach to cross-border disclosure of personal information has been adopted in preference to the current adequacy approach. Under new APP 8, there is a positive requirement on entities to take reasonable steps to ensure the overseas recipient will protect the personal information in a manner which is consistent with the APPs before the cross-border disclosure occurs. APP 8 also sets out a list of exceptions to this requirement. One of these exceptions is if the recipient is subject to a law or binding scheme that will protect the information in a way which is substantially similar to the protection under the APPs *and* there are mechanisms that the individual can assess to enforce that protection.

## Credit Reporting Provisions and New Codes

Five new kinds of credit related personal information (or data sets) are now permitted in the credit reporting system. This means that credit providers will have access to additional personal information to assist them in establishing an individual's credit worthiness. To counter the increased amount of personal information in the system, enhanced obligations and processes dealing with notification, data quality, access and correction and complaints have been included.

New APP codes may be developed by the Commissioner or by APP code developers and will operate in addition to the requirements of the APPs. An APP code will set out how one or more of the APPs are to be applied or complied with. A new Credit Reporting Code of Conduct (CR Code) will also be developed. The CR Code will bind all credit reporting bodies and will set out which credit providers or other entities (e.g. mortgage insurers and trade insurers) will be bound. A breach of an APP Code or the CR Code will be subject to investigation by the Commissioner.

## Australian Privacy Commissioner's Enhanced Powers and Functions

The amendments to the Act will allow the Commissioner to conduct investigations on his own initiative. The Commissioner may investigate an act which may be an interference with an individual's privacy or a breach of APP 1 (Open and Transparent Management of Personal Information). The Commissioner may also make a determination after his investigation which can be enforced by court proceedings. Currently, the Act only allows the Commissioner to make a determination when he is investigating a complaint from an individual.

A further significant change is the extension of the Commissioner's current audit powers from government agencies and credit reporting agencies to private sector organisations. With the reforms, the Commissioner will be able to conduct assessments of private sector organisations to ensure they are maintaining and handling personal information in accordance with the Act.

## Conclusion

Organisations should review their privacy practices, procedures, systems and policies to ensure that they comply with the new APPs and that they are up-to-date. This review must be completed before the end of the nine month transition period when the new APPs come into force. This is particularly important given the Commissioner's new audit and investigatory powers over private sector organisations.

## For further information please contact:

**CHRISTINE ECOB**
***Partner***

T +61 2 8274 9556

christine.ecob@jws.com.au

**TANIA JURIC**
***Special Counsel***

T +61 2 8274 9531

tania.juric@jws.com.au

***Important Disclaimer**: The material contained in this article is comment of a general nature only and is not and nor is it intended to be advice on any specific professional matter. In that the effectiveness or accuracy of any professional advice depends upon the particular circumstances of each case, neither the firm nor any individual author accepts any responsibility whatsoever for any acts or omissions resulting from reliance upon the content of any articles. Before acting on the basis of any material contained in this publication, we recommend that you consult your professional adviser. Liability limited by a scheme approved under Professional Standards Legislation (Australia-wideexcept in Tasmania).*