

Are you across Australian Privacy Law Reforms?

LegalTalk Alert

1 October 2010

pwc

*What would
you like to grow?*

Australian Privacy Law Reforms

Authors: Kathleen Ward, Director and Kimberley Smith, Associate

On 24 June 2010, an Exposure Draft of the Australian Privacy Principles (APPs) was released. The APPs are part of the Australian Government's first-stage response to the Australian Law Reform Commission report 'For Your Information: Australian Privacy Law and Practice (ALRC 108)' (ALRC Report).

The proposed APPs will unify the current National Privacy Principles (which apply to certain private sector organisations) and the Information Privacy Principles (which apply to Commonwealth agencies), and will form part of a new Privacy Act.

What does this mean for your organisation?

If the APPs set out in the Exposure Draft are adopted and enacted as law, private sector organisations and Commonwealth agencies which are subject to the Privacy Act (as amended) will be required to review their existing privacy policies. These reviews should consider whether any amendments are required in light of the new legislation, particularly in relation to the disclosure of personal information to overseas recipients, direct marketing, quality and security of personal information and unsolicited information.

Background

The ALRC Report recommended 295 changes to improve Australia's current privacy framework. Given this large number of recommendations, the Government elected to respond in two stages.

The first stage set out the Government's position in relation to 197 of the recommendations, including:

- developing a single set of privacy principles
- cross-border data flows
- more comprehensive credit reporting and enhanced protection for credit information
- enhancing and clarifying the protections around the sharing of health information
- strengthening the Privacy Commissioner's powers.

The Australian Privacy Principles

The APPs will provide protection for personal information and are designed to regulate the collection, holding, use and disclosure of personal information that is included in records or that is generally available for publication. The following is a summary of the principles contained in the Exposure Draft APPs.

APP 1: Open and transparent management of personal information

Entities must manage personal information in an open and transparent manner.

APP 2: Anonymity and pseudonymity

Individuals must be provided with the option to interact with entities on an anonymous basis or by using a pseudonym. Entities are only obliged to comply with this principle where it is lawful and practicable for the entity to do so.

APP 3 Collection of solicited personal information

Personal information should only be collected where it is reasonably necessary for, or directly related to, one or more of the entity's functions or activities (the Functions Test) and should be collected directly from the individual, unless it is unreasonable or impracticable to do so. This principle also deals with collection of sensitive information. Generally, sensitive information should only be collected where the collection meets the Functions Test and the individual has consented to the collection, subject to the public interest.

APP 4: Collection of unsolicited information

Unsolicited personal information that is received by an entity will still be afforded privacy protections. If the entity could have collected the information under APP3, then it must deal with the information in accordance with that principle. If the entity would not have been permitted to collect the information under APP3, then the entity must take steps to destroy the information.

APP 5: Notification of the collection of personal information

Individuals must be made aware of how, and why, personal information is, or will be, collected and how the collecting entity will deal with their personal information.

APP 6: Use or disclosure of personal information

Entities may use or disclose personal information for the primary purpose for which the information was collected. Personal information should generally only be used for a purpose (other than the primary purpose) if the individual has provided consent, subject to the public interest.

APP 7: Direct marketing

This principle places additional limitations on organisations that use or disclose personal information to promote or sell goods or services directly to individuals and provides a general prohibition against the use or disclosure of personal information for the purposes of direct marketing, unless one of the exemptions applies.

APP 8: Cross-border disclosure

This principle regulates the disclosure of personal information outside of Australia by an entity with Australian links. Generally, prior to disclosing personal information to an overseas recipient, an entity must take reasonable steps to ensure that the recipient does not breach the principle. If the overseas entity is not bound by the APPs, any act by the overseas entity that breaches an APP will be taken to have been committed by the Australian entity (subject to certain exemptions set out in this principle).

Importantly, a cross-border disclosure will be deemed to have occurred where information is accessed by an overseas recipient, whether or not the personal information that is accessed is stored in Australia.

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

The principle ensures that private sector organisations do not refer to individuals according to government identifiers.

APP10: Quality of personal information

This principle protects the quality of personal information which is collected, used or disclosed by entities, and requires such information to be accurate, up-to-date and complete.

APP11: Security of personal information

This principle imposes specific obligations about the protection of personal information from misuse, loss, unauthorised access and interference.

APPS 12 and 13: Access to, and correction of, personal information

These two principles deal with the right of individuals to access personal information that an entity holds about them and to correct the information where the information is inaccurate, irrelevant, incomplete or out-of-date. There are a number of limited circumstances in which an entity may refuse to give an individual access to their own personal information.

Next steps

It is intended that the Government will release three further parts of the new Privacy Act for public consultation as the drafting of each part is completed. Changes may be made to the Exposure Draft APPs as a result of public consultation and the release of further draft legislation.

For further information, please contact your usual PricewaterhouseCoopers contact or:

Andrew Wheeler

Partner

+61 (2) 8266 6401

andrew.wheeler@au.pwc.com

John Cannings

Partner

+61 (2) 8266 6410

john.cannings@au.pwc.com

Stephen Moulton

Partner

+61 (3) 8603 4788

stephen.moulton@au.pwc.com