

REFORM OF AUSTRALIAN PRIVACY LAWS

The Federal Government's proposed reform of Australian privacy laws is in progress with the release of the Exposure Draft Australian Privacy Principles.

If the Exposure Draft Australian Privacy Principles (APPs) become law, businesses will need to:

- review their approach to privacy and redraft privacy policies to provide details of their approach to privacy in light of any new APPs;
- review processes that deal with collecting and disseminating information and transferring personal information overseas;
- review marketing strategies and the impact the APPs would have on marketing; and
- develop ways to deal with individuals who choose to interact with a business anonymously or using a pseudonym.

The APPs are intended to replace the Information Privacy Principles (which apply to Federal Government agencies) and the National Privacy Principles (which apply to certain private sector organisations). A new *Privacy Act* will ultimately be introduced to replicate many of the existing *Privacy Act* principles and refine existing obligations by reference to the APPs.

The release of the Exposure Draft is the first step in the reform process. The Senate Finance & Public Administration Committee is conducting an inquiry into the Exposure Draft and a Companion Guide which has been released to explain the draft APPs.

The committee is seeking submissions from the public which must be lodged by July 27, 2010. This is your chance to provide input on the draft APPs. The committee is not due to report on its findings until July 1, 2011, as there will be additional consultation through the release of more exposure drafts.

The additional exposure drafts that will be released during the next 12 months will focus on:

- introduction of comprehensive credit reporting and enhanced protection for credit reporting information;
- specific privacy protection for information relating to health; and
- the functions and powers of the Australian Information Commissioner.

While there is no timetable for introducing the proposed reforms, it is likely to be late 2011.

The Exposure Draft APP and the Companion Guide are at:

www.aph.gov.au/Senate/Committee/fapa_ctte.

There are 13 draft APPs that would apply to private sector organisations bound by the *Privacy Act*.

APP 1: open and transparent management of personal information. The emphasis is on how information is handled. A business must take reasonable steps to implement practices, procedures and systems that ensure businesses comply with the APPs. A business will need to specify how it discloses personal information to overseas recipients and identify the countries in which recipients are located.

APP 2 – Anonymity and Pseudonymity: Individuals must have the option to identify themselves using a pseudonym or without identifying themselves when dealing with a business, where that is practical.

APP 3 – Collection of Solicited Personal Information: Personal information must not be collected unless it is reasonably necessary for, or directly related to, one or more of the business' functions or activities. The information must be collected directly from an individual. Sensitive information must not be collected except with consent.

APP 4 – Receiving Unsolicited Personal Information: Where an entity receives personal information, that information must be protected even where the business has done nothing to solicit the information. Unsolicited information must be treated in accordance with the APPs.

APP 5 – Notification of the Collection of Personal Information: A business will need to make an individual aware of certain matters at the time personal information is collected. An individual will need to be made aware of how and why personal information is or will be collected and how the collecting entity will deal with the personal information.

APP 6 – Use or Disclosure of Personal Information: Personal information can be used or disclosed for the purpose for which it was collected or a related purpose that the individual would reasonably expect. Exceptions to the rule include consent to use or disclosure by the individual, or disclosure which is reasonably necessary for the defence of a legal or equitable claim.

APP 7 – Direct Marketing: Extra limitations will be imposed on businesses that use or disclose personal information to promote or sell goods or services directly to individuals. This principle will not apply to electronic marketing or telemarketing which is governed by the *Spam Act* and the *Do Not Call Register Act*. Personal information can be used in marketing if the individual would reasonably expect the information supplied to be used that way or with the individual's consent. The individual will have the right to "opt out" from marketing.

APP 8 – Cross-Border Disclosure of Personal Information: Businesses must ensure the APPs cannot be avoided by disclosing personal information to a recipient outside Australia. Businesses will need to take steps to ensure an overseas recipient of information takes reasonable steps to ensure there is no breach of the APPs in relation to personal information. Appropriate arrangements need to be put in place before disclosure of information overseas. While the APPs cannot apply to overseas entities, any breach of an APP by an overseas entity will be taken to have been committed by the Australian entity that disclosed the information overseas.

APP 9 – Adoption, Use or Disclosure of Government-Related Identifiers: Individuals must not be identified by identifiers such as Medicare numbers. The intention is to ensure identifiers issued by government agencies are not used as a de-facto national identity number.

APP 10 – Quality of Personal Information: Reasonable steps are required to ensure personal information collected, used or disclosed is accurate, up to date and complete.

APP 11 – Security of the Personal Information: In line with international best practice, personal information must be kept securely. Reasonable steps must be taken to protect information from misuse, interference, loss, unauthorised access, modification and disclosure. Personal information must be destroyed if it is no longer needed for the purposes for which it was collected.

APP 12 – Access to Personal Information: Individuals will have the right to access their information. Individuals will have the right to request that information which is inaccurate, irrelevant or out of date is corrected.

APP 13 – Correction of Personal Information: An obligation is imposed on a business to correct personal information if it is inaccurate, out of date, incomplete or irrelevant.

Conclusion

The reform of Australian privacy laws is in progress. The review will progress over the next 12 months. The release of additional exposure drafts will provide businesses with the opportunity to provide input to the Senate Committee on the proposed changes.

For now, businesses do not need to take any action unless they wish to make a submission to the Senate Committee.

David Newey
Gillis Delaney Lawyers
T: +61 2 93941111
E: dtm@gdlaw.com.au