



# mertons

corporate governance specialists

## Mertons' Update – Australian Privacy Principles

**From 12 March 2014 the Australian Privacy Principles (APPs) will apply to most organisations.**

This update is intended to provide you with a summarised guide to recent or upcoming corporate governance matters. If you would like further information or assistance with how it may affect your business, please contact:

**Mark Licciardo**  
Managing Director  
ph: 03 8689 9997  
e-mail: [markl@mertons.com.au](mailto:markl@mertons.com.au)

**Matt Rowe**  
Corporate Governance Advisor  
ph: 03 8689 9997  
e-mail: [mattr@mertons.com.au](mailto:mattr@mertons.com.au)

### Executive Summary

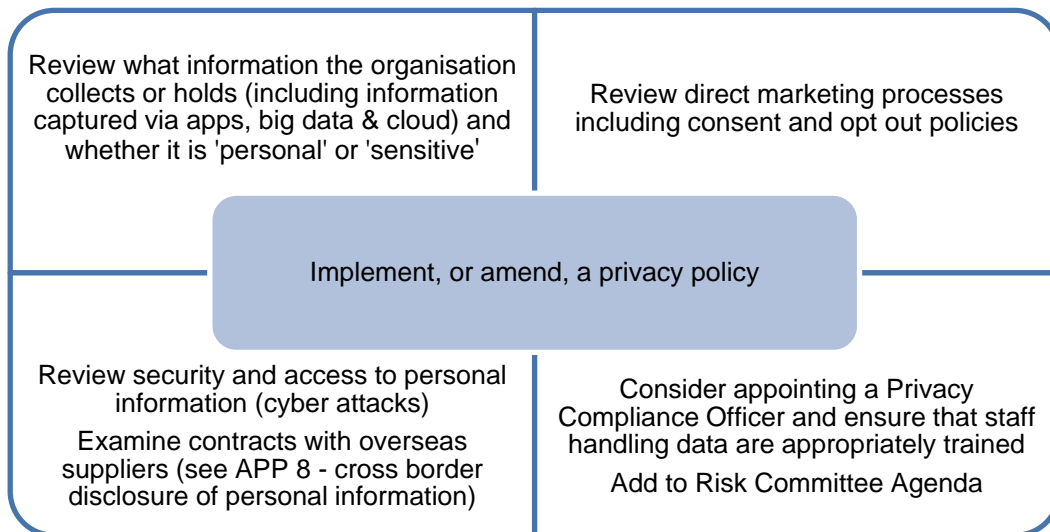
12 March 2014 marked the replacement of the National Privacy Principles and Information Privacy Principles with the Australian Privacy Principles (APPs) from Schedule 1 of the Privacy Amendment (enhancing Privacy Protection) Act 2012. The thirteen APPs are detailed in the attached notes section.

#### Who is covered by the APPs?

Any Australian organisation with an annual turnover of over \$3 million will be considered an 'APP Entity'. Small business operators (organisations with a turnover under \$3 million) may also be caught by the exemptions (see notes section).

For those organisations caught by the annual turnover threshold, it would be prudent for the Board to allocate sufficient resources to ascertain the level of impact and the appropriate response which should be summarised in a Privacy Policy. Privacy Policies should be reviewed on a regular basis by the Board or Risk Committee or when an organisation acquires or moves into new business areas. Risks of not doing so include financial penalties (up to \$340,000 for individuals and \$1.7 million for corporations), legal costs of any prosecution and reputational damage.

### Next Steps



Mertons can assist you preparing and implementing your Privacy Policy.

**A Small Business Operator** is an individual (including a sole trader), body corporate, partnership, unincorporated association or trust that has an annual turnover of \$3 million or less for a financial year, unless an exception applies (s 6D). If an exception (as noted below) applies to a small business operator it may be deemed an APP Entity. The exceptions include businesses that:

- provide a health service and hold health information other than in an employee record
- disclose personal information about another individual for a benefit, service or advantage, or provide a benefit, service or advantage to collect personal information about another individual from anyone else, unless they do so with the consent of the individual or are required or authorised by or under legislation to do so
- are contracted service providers for a Commonwealth contract.

### APP Principles

Number	Principle, <sup>1</sup> key items to note for an APP entity:
1.	<b>open and transparent management of personal information</b> must have a clearly expressed and up to date policy regarding the management of personal information ie. a Privacy Policy
2.	<b>anonymity and pseudonymity</b> must offer individuals the option of not identifying themselves or of using a pseudonym
3.	<b>collection of solicited personal information</b> must not collect personal information unless the information is reasonably necessary for one or more of the entity's functions or activities
4.	<b>dealing with unsolicited personal information</b> is required to consider the content of information and if necessary destroy or de-identify the information
5.	<b>notification of the collection of personal information</b> must take such steps as reasonable to notify the individual as to a range of matters including identity and contact details of the APP entity
6.	<b>use or disclosure of personal information</b> must obtain consent when disclosing personal information
7.	<b>direct marketing</b> must provide the ability for the individual to 'opt-out' of marketing and/or provide source of information
8.	<b>cross-border disclosure of personal information</b> must recognise that in certain circumstances, an act done, or a practice engaged in by the overseas recipient is taken to have been done, or engaged in by the APP entity
9.	<b>adoption, use or disclosure of government related identifiers</b>
10.	<b>quality of personal information</b> must take reasonable steps to ensure personal information collected is accurate, up-to-date and complete
11.	<b>security of personal information</b> must protect from misuse, interference and loss from unauthorised access, modification and disclosure
12.	<b>access to personal information</b> must have procedures for giving an individual access to their personal information
13.	<b>correction of personal information</b> must have procedures for giving an individual ability to correct their personal information

**Personal information** is defined as any 'information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not (s 6(1)).

Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details, employment details and commentary or opinion about a person.

**Sensitive information** is a subset of personal information and is defined as:

- information or an opinion (that is also personal information) about an individual(s):
  - racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association.

Disclaimer: The content in this Mertons Bulletin is intended only to provide a summary and general overview on matters of interest. It is not intended to be comprehensive nor does it constitute legal advice. We attempt to ensure that the content is current but we do not guarantee its currency. You should seek legal or other professional advice before acting or relying on any of the content.

<sup>1</sup> Source: Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012