

31 January 2014

### Summary of Australian Privacy Principles (APPs)

- **APP1 – Open & transparent management of personal information**  
APP entities must take reasonable steps to implement practices, procedures and systems that ensure compliance with the APPs. This may include staff training, or establishing procedures to identify and manage privacy risks. This includes having a clearly expressed and up to date APP privacy policy and a system for handling privacy enquiries and complaints.
- **APP2 – Anonymity and pseudonymity**  
Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Some exceptions apply, for example where it would be impracticable for the organisation to deal with an unidentified individual.
- **APP3 – Collection of solicited personal information**  
Outlines new rules that apply to collection practices and notices when collecting personal information and/or sensitive information (such as health information). Higher standards are applied to the collection of sensitive information. The collection of personal information must be “reasonably necessary” for one or more of an organisation’s functions or activities.
- **APP4 – Dealing with unsolicited personal information**  
Outlines new rules on how to deal with unsolicited personal information, including when this information must be destroyed or de-identified.
- **APP5 – Notification of the collection of personal information**  
Deals with when, and in what circumstances an APP entity that collects personal information must notify an individual of when collecting their personal information. These matters include who the organisation is and how to contact it, the purpose of the collection, the consequences of non-collection and the complaint handling process.
- **APP6 – Use or disclosure of personal information**  
Outlines new rules as to when personal and sensitive information can be used or disclosed.

*Insight. Commitment*

#### Mackay Office

Level 1, City Court, 78 Victoria Street, Mackay  
PO Box 1035, Mackay Qld 4740

P 07 4911 0500 | F 07 4911 0599 | E [mail@kellylegal.com.au](mailto:mail@kellylegal.com.au)  
[www.kellylegal.com.au](http://www.kellylegal.com.au)

#### Brisbane Office

Level 4, Bank of NSW Chambers, 33 Queen Street, Brisbane  
PO Box 13531, George Street, Brisbane Qld 4003

P 07 3179 2700 | F 07 3179 2799 | E [mail@kellylegal.com.au](mailto:mail@kellylegal.com.au)  
[www.kellyfamilylaw.com.au](http://www.kellyfamilylaw.com.au)

Disclaimer: The contents of this publication are not intended as professional legal advice. You should obtain independent legal advice before relying or acting on any statements, recommendations or opinions contained in this publication. Kelly Legal Pty Ltd cannot accept any liability or loss occurring as a result of anyone acting in reliance on any material contained in this publication.

Kelly Legal Pty Ltd ABN 15 125 481 361 | Individual liability limited by a scheme approved under professional standards legislation

© 2013 Kelly Legal Pty Ltd

- **APP7 – Direct marketing**

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met. The new rules will require organisations to review their direct marketing practices, procedures and systems, including whether individuals are provided with an easy way to opt out of receiving direct marketing. This is subject to the operation of other direct marketing legislation, e.g. the *Spam Act 2003*.

- **APP8 – Cross border disclosure of personal information**

Details the steps that an APP entity must take to protect personal information before it is disclosed overseas. Introduces an accountability approach for cross border disclosure and organisations may be accountable for a breach of APP's by overseas recipients.

- **APP9 – Adoption, use or disclosure of government related identifiers**

Outlines the new exceptions to the general prohibition against the adoption, use or disclosure of government related identifiers (e.g. a unique combination of letters and numbers used by a government agency, such as a Medicare number).

- **APP10 – Quality of personal information**

Requires an APP entity to take reasonable steps to ensure that the personal information they collect, use or disclose is up to date, complete and accurate, and relevant for the purpose of the use or disclosure.

- **APP11 – Security of personal information**

APP entities must take reasonable steps to protect personal information it holds from misuse, interference (including measures to protect against computer attacks), loss and from unauthorised access, modification or disclosure. An entity has an obligation to destroy or de-identify personal information in certain circumstances.

- **APP12 – Access to personal information**

There are new rules on how an APP entity must respond to a request for access to and correction of personal information. Requests must be responded to within a reasonable timeframe and in the requested manner, where practicable. Charges for access to personal information must not be excessive or apply to the making of the request.

- **APP13 – Correction of personal information**

Outlines an APP entity's obligations regarding the correction of personal information, even if it has not received a request from an individual.