

File Name: 2013/42

21 October 2013

Draft Australian Privacy Principles (APP) Guidelines – second tranche

ASFA considers that the second tranche of the draft *Australian Privacy Principle Guidelines*, covering the Australian Privacy Principles (“APPs”) 6 to 11 (“the draft Guidelines”) provides clear and useful guidance for organisations as they move toward compliance with the privacy reforms. However, ASFA is concerned that the consultation on the guidelines is still at a preliminary stage, with less than five months until the commencement of the reforms.

ASFA’s submission focussed on the particular impacts of the draft Guidelines on the superannuation industry, in which large volumes of personal information are required to be collected, used and disclosed as part of the administration of members’ superannuation monies. ASFA’s recommendations included:

- Providing examples of how the APPs apply in the context of the provision of financial services by an APP entity to an individual;
- Confirming that simply accessing and/or searching within a record that contains an item of personal information does not result in the ‘use’ of every item of information contained in that record;
- Using examples that more clearly distinguish between an APP entity’s primary and secondary purposes for collecting information;
- Acknowledging that APP 7 will continue to apply to direct marketing involving telecommunications and electronic communication methods governed by the *Do Not Call Register Act* and the *Spam Act*, where an exemption applies under those Acts.
- Updating current guidance on the interaction between the *Privacy Act* and the *Spam Act* to reflect the new APPs and to also cover the *Do Not Call Register Act*;
- Clarifying the examples of what does, and does not, constitute direct marketing;
- Explaining when the use of cloud computing services might constitute a ‘disclosure’ rather than a ‘use’ of personal information, and providing specific guidance on compliance with the APPs for entities who utilise cloud computing services;
- Clarifying the expectation that a binding contract will be in place between the APP entity and an overseas recipient to whom personal information is disclosed, and providing other examples of ‘reasonable steps’ an entity can take to ensure the overseas recipient complies with the APPs;
- Providing at least a baseline level of information about the privacy protections offered in overseas jurisdictions, to help entities comply with their obligations under APP 8;
- Including specific reference to the Foreign Accounts Tax Compliance Act (FATCA), and providing more detailed guidance for APP entities about the interaction between FATCA and their privacy obligations;
- Including AUSTRAC as an example of an ‘enforcement body’ to whom information can be disclosed, and providing a detailed example involving disclosure to AUSTRAC of personal information, including government related identifiers; and
- Confirming that where a government related identifier, included in a paper or electronic copy of a document used for identification purposes, is retained as part of an individual’s record held by an APP entity, the entity does not ‘use’ the identifier in contravention of APP 9.2 merely by accessing and searching within the individual’s record.