The Association of Superannuation Funds of Australia Limited
ABN 29 002 786 290
ASFA Secretariat
PO Box 1485, Sydney NSW 2001
p: 02 9264 9300 (1800 812 798 outside Sydney)
f: 1300 926 484
w: www.superannuation.asn.au

File Name: 2013/39

20 September 2013

Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001

Email: consultation@oaic.gov.au

Dear Commissioner,

**Draft Australian Privacy Principles (APP) Guidelines – first tranche**

The Association of Superannuation Funds of Australia (ASFA) is pleased to provide this submission in response to the first tranche of the draft *Australian Privacy Principle Guidelines*, covering the 'general matters' (chapters A to D) and Australian Privacy Principles ("APPs") 1 to 5 (Chapters 1 to 5) ("the draft Guidelines").

## ABOUT ASFA

ASFA is a non-profit, non-political national organisation whose mission is to protect, promote and advance the interests of Australia's superannuation funds, their trustees and their members. We focus on the issues that affect the entire superannuation industry. Our membership, which includes corporate, public sector, industry and retail superannuation funds, plus self-managed superannuation funds (SMSFs) and small APRA funds through its service provider membership, represent over 90% of the 12 million Australians with superannuation.

## GENERAL COMMENTS

We have reviewed the draft Guidelines from the perspective of superannuation funds, who will be APP entities under the recent amendments to the *Privacy Act 1988* ("the Act"), and their members. The superannuation environment is highly regulated, with large volumes of personal information required (directly or indirectly) by law to be collected, used and disclosed as part of the administration of members' superannuation monies. However, while the focus of our submission is on the particular impacts of the draft Guidelines on the superannuation industry, many of our comments will also apply to other industries which are subject to a high degree of regulation.

In general terms, we consider that the draft Guidelines provide clear and useful guidance for organisations as they move toward compliance with the privacy reforms. To that end, we strongly recommend that every effort is made to finalise and publish the Guidelines as soon as possible. We note that there are now less than six months until the commencement of the reforms, and there are a further two stages of consultation to be conducted in relation to the draft Guidelines.

**Recommendation 1:**
That the Commissioner releases the outstanding tranches of the draft Guidelines as soon as possible, and publishes the final Guidelines well before 12 March 2014.

**SPECIFIC COMMENTS**

Whilst ASFA broadly welcomes the recent amendments to the Act we do have some concerns in relation to specific aspects of the draft Guidelines. These are set out below.

## 1. Chapter B – key concepts

### *1.1 Paragraphs B.32 – B.33– Bundled consent*

Paragraph B.33 states that the practice of 'bundling' consent "has the potential to undermine the voluntary nature of the consent".

Whilst we acknowledge that this may be the case in some circumstances, we submit that bundling of consent is often necessary in practice, in order to avoid confusing or inconveniencing the individual whose information is being collected and to prevent inefficiencies.

In the superannuation industry (and indeed the broader financial services industry), a provider will typically collect some relatively commonplace items of personal information, which are then used and/or disclosed for a number of different purposes, many of which are required or authorised by law. (See comments under section 3.1 below for a specific example in the context of the collection, use and disclosure of a fund member's date of birth.) In carrying out these purposes the provider may need to disclose the information to a range of outsourced service providers – for example, administration ('back office') service providers, insurers, actuaries, technology providers, mail-houses, regulators and complaints handling bodies and, in relation to members who seek to roll over their benefit, other superannuation funds.

It is currently common practice for the provider to obtain a single, 'bundled' consent to the collection of such information. Requiring the provider to request separate consents – in effect purporting to allow the member to 'pick and choose' the uses and/or disclosures for which they will consent – is highly impractical, for a number of reasons:

- In some cases, the member may attempt to withhold their consent to the collection of information that is required or authorised by law, which is likely to cause confusion;
- It would significantly increase the length and complexity of the collection notification;
- It would require the provider to develop and maintain the capacity to record and store multiple consents for individual items of personal information.

> **Recommendation 2:**
> That the wording of paragraph B.33 be amended to reflect that bundling of consents may be appropriate in some cases.

### *1.2 Paragraph B.34 - Informed*

Paragraph B.34 states that an APP entity "should give information directly to the individual about how their personal information is to be handled, in a way that the individual understands" (our emphasis). This statement does not appear to contemplate the situation where an APP entity collects an individual's personal information from another entity, in circumstances where that other entity has provided the notification necessary under APP 5.

In particular, the statement in paragraph B.34 appears to be inconsistent with the last bullet point in paragraph 5.5, which describes the 'reasonable steps' an APP entity could consider taking in order to notify the individual of 'APP 5 matters' in these terms:

> If the entity collects personal information from another entity – confirming whether the other entity has provided the relevant APP 5 notice to the individual, or whether the individual was otherwise aware of the APP 5 matter at the time of collection.

**Recommendation 3:**
That the wording of paragraph B.34 be amended to reflect that it may be permissible in the circumstances for the necessary information to be given to the individual by another entity.

### *1.3 Paragraph B.37 - Capacity*

The draft Guidelines provide useful suggestions about how an APP entity should proceed when dealing with an individual who lacks the capacity to consent to the collection of their personal information. However, ASFA is concerned that the draft Guidelines might be interpreted as requiring an APP entity to assess an individual's capacity prior to seeking to collect their information. This is inconsistent with current business practice, where capacity to consent is presumed unless and until the entity seeking to rely on the consent is put on notice that capacity may be lacking.

We note that the current *Guidelines to the National Privacy Principles* explicitly recognise such a presumption of capacity (refer page 22):

> Only a competent individual can give consent although an organisation can ordinarily assume capacity unless there is something to alert it otherwise.

ASFA submits that the existence of a presumption of capacity should be specifically recognised in the APP Guidelines.

**Recommendation 4:**
That the wording of paragraph B.37 be amended to note that an APP entity may ordinarily presume an individual's capacity to consent to the collection of their personal information, in the absence of indications to the contrary.

### *1.4 Paragraphs B.87 – B.89 – Recognised external dispute resolution scheme*

New Section 35A of the Act gives the Commissioner the power to recognise external dispute resolution schemes ("EDR schemes"). New paragraphs 41(1)(dc) and (dd) provide that the Commissioner may decide not to investigate a complaint by an individual about an act or practice of an APP entity if satisfied that the act or practice is being dealt with by a recognised EDR scheme, or that it would be more effectively or appropriately dealt with by a recognised EDR scheme. Membership of a recognised EDR scheme is not mandatory, unless an APP is a credit provider or a credit reporting body.

Whilst these represent significant changes to the current regulatory framework for privacy in Australia, at this point there is relatively little information available to help APP entities understand the full implications, and the three paragraphs about EDR schemes in the draft Guidelines do little to advance understanding of these matters. At this point it is not even clear whether there are likely to be EDR schemes recognised to deal with privacy complaints that are not credit-related.

This is of concern because APP entities are now in the midst of preparing to comply with the APPs from 12 March 2014. This includes:

- APP 1.2, which requires an APP entity to take reasonable steps to implement practices, procedures and systems that will enable it to deal with inquiries or complaints from individuals about its compliance with the APPs; and
- APP 1.4(e), which requires an APP entity to include in its APP privacy policy details of how an individual may complain about a breach of the APPs, and how the APP entity will deal with such a complaint.

Without further clarity around the use of EDR schemes, it will be difficult for APP entities to finalise these matters.

We note that the Commissioner intends to publish separate *Guidelines for recognising external dispute resolution schemes under section 35A of the Privacy Act 1988* ("EDR scheme guidelines"), consultation on a draft of those guidelines having concluded on 30 August 2013. However, those Guidelines are very much focussed on the criteria the Commissioner will apply in determining whether to recognise an EDR scheme. They do not consider the matter from the perspective of an APP entity.

In particular, the EDR scheme guidelines do not (and are not intended to) provide APP entities with information that would help them to make decisions regarding potential membership of an EDR scheme. In this respect, it is worth noting that membership of an EDR scheme will be a novel development for many APP entities, and will require careful consideration. APP entities will need information to assist them through this process, for example:

- The types of EDR schemes which are likely to seek recognition by the Commissioner under section 35A, and will therefore be available for selection by APP entities;
- The implications of membership of a recognised EDR scheme for the APP entity and for an individual whose complaint is heard by the EDR scheme;
- The impact on the complaints process required under APP1.2 where an APP entity does, or does not, become a member of a recognised EDR scheme.

**Recommendation 5:**
That the Commissioner:

- releases general guidance directed at APP entities about the intended operation of recognised EDR schemes; and
- finalises the draft *Guidelines for Recognising External Dispute Resolution Schemes under s35A of the Privacy Act* as soon as possible.

### *1.5 Paragraph B.102 – meaning of 'Australian law'*

Paragraph B.102 defines 'Australian law' as including "an Act of the Commonwealth, or of a State or Territory" and "regulations or any other *legislative* instrument made under such an Act" (our emphasis). In contrast, the definition of "Australian law" inserted into section 6(1) of the Act refers to "regulations, or any other instrument" made under an Act" (our emphasis).

The term 'legislative instrument' has a specific technical meaning under the *Legislative Instruments Act 2003*. In contrast, the term 'instrument' has a more general meaning and could be interpreted as including instruments that are not 'legislative instruments' as defined.

It is not clear whether the use of the term 'legislative instruments' in the draft Guidelines is inadvertent, or rather an attempt to qualify the meaning of' Australian law' as set out in section 6(1). This lack of clarity presents difficulties for APP entities in determining and meeting their obligations under the APPs.

For example, the Australian Taxation Office ("ATO") issues a number of 'electronic reporting specifications' which require superannuation fund providers to report detailed information regarding their members (see specific examples raised under 2.1 in the context of the notification required to be given to an individual regarding the collection of personal information). These specifications are 'approved forms' made under legislation, and arguably would fall within the ordinary meaning of the term 'instruments', but they are not 'legislative instruments' in the strict sense. Are these specifications to be considered 'Australian law'?

**Recommendation 6:**
The definition of 'Australian law' in paragraph B.102 should be revised and made consistent with the definition in section 6(1) of the Act.

## 2. Chapter 1 – APP 1 – open & transparent management of personal information

### *2.1 Paragraphs 1.8 – 1.30 – developing an APP privacy policy*

We note that new APPs 1.3 – 1.4 are significantly more prescriptive about the content of an APP entity's privacy policy than is the current NPP 5.1.

The draft Guidelines provide useful clarification of the information that APP entities should consider including in their APP privacy policy, in order to address each requirement of APP 1.4. However, the overall impression gained from reading paragraphs 1.15 – 1.30 is that in order to comply with the Guidelines, an APP privacy policy will be a reasonably lengthy and detailed document.

It is difficult to reconcile that outcome with the comment in paragraph 1.8 that the APP privacy policy "should be written in a style and length that makes it easy to understand and suitable for web publication". Similarly, it appears to be somewhat at odds with concerns about the observed length of current privacy policies, expressed in the media release *'Privacy Commissioner: Website privacy policies are too long and complex*', dated 14 August 2013.

> **Recommendation 7:**
> That the Guidelines provide greater clarity around what is considered to be an appropriate length for an APP privacy policy.

### *2.2 Paragraphs 1.25 – 1.28 – likely overseas disclosures (APP 1.4(f) and 1.4(g))*

Taken together, APP 1.4(f) and 1.4(g) require an APP entity to indicate in its APP privacy policy whether the APP entity is likely to disclose personal information to overseas recipients and, if so, the countries in which such recipients are likely to be located, if it is practicable to specify those countries in the policy.

We note that the use of cloud services will present particular challenges for APP entities in complying with these requirements. A significant level of due diligence may be required in order to specify, with any level of certainty, the countries to which personal information may be disclosed 'through the cloud'.

Whilst we understand that the Act and Guidelines aim to be 'technology neutral' in language, we submit that additional guidance – perhaps in a separate information sheet or similar – regarding the specific privacy considerations raised by the use of cloud services would be beneficial.

> **Recommendation 8:**
> That the Commissioner considers providing specific guidance on compliance with the APPs for APP entities who utilise cloud computing services.

## 3. Chapter 5 – APP 5 – notification of the collection of personal information

### *3.1 Paragraphs 5.12 & 5.13 – if the collection is required or authorised by law (APP 5.2(c))*

While paragraphs 5.12 and 5.13 specifically address situations where the *collection* of information is required or authorised by law, many laws which do not directly or positively require or authorise the *collection* of certain information by an entity nonetheless contain a direct or positive obligation to *use or disclose* it. In such cases, the obligation to collect the information must be seen as implicit. That is, the information cannot be used or disclosed if it has not first been collected.

Paragraph 5.13 states the view that where the collection of personal information is required or authorised by law, the notification of the collection of personal information should "name the particular law relied upon, and not the range of laws available to the entity to collect personal information, nor a generic description (such as 'taxation law')."

This is generally consistent with the wording of APP 5.2(c), which refers to a notification "including the name of the Australian law… that requires or authorises the collection". However, it represents a significant policy change when compared to the current National Privacy Principle, NPP 1.3(e), which refers more generally to the organisation taking reasonable steps to ensure the individual is aware of "any law that requires the particular information to be collected". The Guidelines to the National Privacy Principles (refer page 31) specifically allow a general description of the relevant law to be given:

> NPP 1.3(e) Informing individuals of any legal obligation to collect
> This means an organisation must take reasonable steps to tell the individual about any law that requires the individual to provide, or the organisation to collect, personal information in the particular situation. In describing the law the organisation need not specify the exact piece of legislation (although it would be desirable to do this where possible). A statement like 'taxation law requires us to collect this' would ordinarily be adequate.

We acknowledge that the wording of APP 5.2(c) is more specific than NPP 1.3(e). However, we submit that if the approach to notification described in paragraph 5.13 is applied strictly in highly regulated industries such as superannuation, it is likely to produce a notification that is *less* – rather than more – meaningful to the individual whose information is being collected.

By way of illustration, a superannuation fund provider typically collects the date of birth of a member or prospective member. This is used and disclosed for a range of purposes which are subject to legislative obligations, including:

i) The *Superannuation Industry (Supervision) Regulations 1994*, which require the provider to be satisfied regarding a member's age before accepting contributions or making a benefit payment;

ii) The *Income Tax Assessment Act 1997*, which require knowledge of the member's age in order to apply the appropriate tax treatment to benefits;

iii) The *Anti-Money Laundering & Counter-Terrorism Rules Instrument 2007 (No. 1)*, which requires collection of 'Know Your Client' information, including the individual's date of birth, before the provider may pay a cash benefit to the member;

iv) The *Superannuation Data and Payment Standards 2012* (a legislative instrument made by the ATO under the *Superannuation Industry (Supervision) Act 1993*), which requires information including the member's date of birth to be reported where a member's benefit is rolled over between funds;

v) The *Superannuation (Unclaimed Money and Lost Members) Act 1999*, which requires providers to take certain actions where a member has reached 'eligibility age' (currently age 65), and also to report information including a member's date of birth to the ATO in accordance with the *Lost members statement (LMS) electronic reporting specification* and the *Unclaimed superannuation money (USM) statement electronic reporting specification* (issued by the ATO as approved forms under the *Superannuation (Unclaimed Money and Lost Members) Act 1999*);

vi) The *Taxation Administration Act 1953*, which requires providers to report information for all fund members, in accordance with the *Member contributions statement (MCS) electronic reporting specification*, including their dates of birth (the specification is an approved form issued by the ATO under the *Taxation Administration Act 1953*).

Currently, superannuation providers use a generic description for the above list of legislation and instruments, in accordance with the Guidelines for compliance with NPP 1.3(e). For example, the collection statement might say something along these lines: "We are required or authorised to collect this information under a number of superannuation and taxation related laws". In contrast, strict compliance with paragraph 5.13 would appear to require a fund to separately name each piece of 'Australian law' noted above. (We note that it is unclear from the draft Guidelines whether the 'electronic reporting specifications' noted above would be considered 'Australian law' - see our comments regarding the distinction between 'legislative instruments' and 'instruments' under section 1.5 above.

This would produce a very detailed notification in respect of the collection of a single piece of personal information. If this process is repeated for all other items of personal information that are typically required in order to administer a member's superannuation account, the resulting notification would be extremely lengthy and complex. Rather than inform the individual, we submit that this approach is more likely to confuse and overwhelm.

Further, the outcome would seem to be inconsistent with the requirement in paragraph 1.14 that an entity's APP privacy policy should "avoid jargon… and legalistic expressions". If "legalistic" terminology is inappropriate in a privacy policy, it is equally inappropriate, in our view, for a collection notification under APP 5 to contain a long list of legislative references.

We note also that the approach required by paragraph 5.13 will be difficult to maintain on an ongoing basis, due to the frequent amendment of existing legislation, passage of new legislative requirements and occasional repeal of legislation. This may result in:

i) new (additional) items of personal information being collected;

ii) new required uses/disclosures of information that has already been collected under other law, and/or

iii) the repeal of a law under which personal information was previously authorised or required to be collected, even though it may still be authorised by another piece of legislation.

We note that view stated in paragraph 5.7 of the draft Guidelines that "it may be reasonable for an APP entity to notify some but not all of the APP 5 matters". We recommend that the Guidelines include a specific acknowledgement that it may be reasonable, in highly regulated industries, for an APP entity not to notify an individual in specific terms about all of the matters stated in APP 5.2(c). We note that it is always open for an individual to request more specific information if they require it, and that APP 1.2 specifically requires an APP entity to implement practices, procedures and systems to enable them to deal with inquiries from individuals about their compliance with the APPs.

**Recommendation 9:**
That paragraph 5.13 be amended to specifically note that in some highly regulated industries (for example superannuation), it may be reasonable for the APP entity to use generic, descriptive terms rather than specifically identify the Australian law(s) which require(s) or authorise(s) the collection of personal information.

Each of the three scenarios above would require amendment of a provider's collection notification going forward. Where an item of information previously collected from an individual is 're-collected', the individual will, appropriately, receive an updated collection notification. However, in some cases an item of information that is collected at one point in time will continue to be used and disclosed without 're-collection' from the individual. We presume that in such cases the provider would not be required to notify the individual about the change to the law authorising or requiring the use or disclosure of the information in question. Any such requirement would, in our view, impose an inappropriately onerous burden on the provider.

We note that scenario (ii), in particular, is so common in the superannuation industry that some legislation actually seeks to pre-empt it. For example, while the *Superannuation Industry (Supervision) Act 1993* contains detailed rules regarding the purposes for which superannuation providers may use the Tax File Numbers ("TFNs") of members, it specifically recognises that these purposes may change over time, by referring to the quotation of a TFN by a member "in connection with the operation or the possible future operation of this Act and the other Superannuation Acts" (our emphasis, see for example section 299H). Similarly, the *Superannuation Industry (Supervision) Tax File Number approval No. 1 of 2007*, which details the information that must be given to a fund member or prospective member before they quote their TFN, refers to the provider being authorised to collect the member's TFN, "which will only be used for lawful purposes. These purposes may change in the future as a result of legislative change."

**Recommendation 10:**
That the Guidelines make it clear that where there has been a change to the Australian law requiring or authorising the collection, use or disclosure of an item of personal information, that need only be notified to an individual when information is next collected, and that notification is not required for continued use and/or disclosure of information previously provided.

### *3.2 Paragraphs 5.24 – 5.28 – Cross-border disclosure (APP 5.2(i) and (j))*

APP 5.1(i) and (j) effectively require that, where an APP entity is likely to disclose personal information to overseas recipients, it must include in the collection notification to the individual details about the countries in which such recipients are likely to be located, if it is practicable to specify those countries in the notice or otherwise make the individual aware of them.

ASFA considers that APP entities that use cloud computing services will face particular challenges in complying with this and other APPs regarding cross-border disclosures (see comments under 2.2 above). Given the increasing take-up of cloud services, specific guidance on these matters would be welcomed.

> **Recommendation 11:**
> That the Commissioner considers providing specific guidance on compliance with the APPs for APP entities who utilise cloud computing services.

* * * * *

I trust that the information contained in this submission is of value. If you have any queries or comments regarding the contents of our submission, please contact Senior Policy Adviser, Julia Stannard on (03) 9225 4027 or via e-mail jstannard@superannuation.asn.au.

Yours sincerely

Fiona Galbraith
Director, Policy