INSURANCE COUNCIL OF AUSTRALIA

The Privacy Commissioner
Office of the Australian Information Commissioner
GPO Box 5218
SYDNEY NSW 2001

By email: consultation@oaic.gov.au

21 October 2013

Dear Commissioner

DRAFT AUSTRALIAN PRIVACY PRINCIPLES GUIDELINES 6 - 11

The Insurance Council of Australia[1] (Insurance Council) appreciates the opportunity to provide comments on the second tranche of the draft guidelines (Draft Guidelines) on the Australian Privacy Principles (APPs) 6 - 11. Our comments in the **Attachment** should be read in conjunction with the Insurance Council's previous comments on APPs 1 – 5 (20 September 2013).

Similarly to those previous comments, we believe these Draft Guidelines:

- appear to discount cost as a relevant consideration of what is reasonable or practicable (for example, 7.25, 7.39 and 11.5);
- should be made sufficiently flexible for entities to comply and not take an unnecessarily complex approach (for example 7.20 and 7.29: the means of opt-out messages).

With commencement of the reforms on 12 March 2014, it is critical that the Guidelines are finalised as soon as possible to be a useful resource for our members. Should finalisation be delayed, the Office of the Information Commissioner should recognise the impact this may have on entities implementing the processes suggested by the final guidance.

[1] The Insurance Council of Australia is the representative body of the general insurance industry in Australia. Our members represent more than 90 percent of total premium income written by private sector general insurers. Insurance Council members, both insurers and reinsurers, are a significant part of the financial services system. June 2013 Australian Prudential Regulation Authority statistics show that the private sector insurance industry generates gross written premium of $39.9 billion per annum and has total assets of $118.1 billion. The industry employs approximately 60,000 people and on average pays out about $106 million in claims each working day.

Insurance Council members provide insurance products ranging from those usually purchased by individuals (such as home and contents insurance, travel insurance, motor vehicle insurance) to those purchased by small businesses and larger organisations (such as product and public liability insurance, professional indemnity insurance, commercial property, and directors and officers insurance).

Insurance Council of Australia Limited ABN 50 005 617 318
PO Box R1832 Royal Exchange NSW Australia 1225
t +61 2 9253 5100 f +61 2 9253 5111
www.insurancecouncil.com.au

INSURANCE COUNCIL OF AUSTRALIA

If you have any questions or comments in relation to our submission, please contact John Anning, the Insurance Council's General Manager Policy, Regulation Directorate, on tel: (02) 9253 5121 or email: janning@insurancecouncil.com.au.

Yours sincerely

Robert Whelan
Executive Director & CEO

ATTACHMENT

AUSTRALIAN PRIVACY PRINCIPLES GUIDELINES

Chapter 6 - APP 6: use or disclosure of personal information

(6.17) APP 6.1(a) permits an APP entity to use or disclose personal information for a secondary purpose where the individual has consented to the use or disclosure.

The Insurance Council submits the Draft Guidelines should make it clear that allowable uses, including those relating to a secondary purpose, made pursuant to the original provision of consent cannot be undone by the subsequent withdrawal of consent. The Insurance Council refers to its previous submission addressing this point.

(6.12) The primary purpose of collection should be determined on a case-by-case basis and will depend on the circumstances. However in general, 'primary purpose' should be construed narrowly. This ensures that individuals understand and retain some control over how their personal information is used and disclosed.

The Insurance Council notes the concept of primary purpose is to be construed narrowly. This is the first time this expression has been used and we are unclear as to how the narrow construction ensures "individuals understand and retain some control" over how the personal information is used and disclosed. We are also concerned that a narrow definition may be problematic and unreasonably restrict the definition of a "primary purpose" while creating an unrealistic interpretation of secondary purpose. For example, where the primary purpose is provision of insurance there may be services that are ancillary to the actual underwriting, such as advising, contact where services change and claims processing. We would broadly interpret the primary purpose of underwriting a risk to include the services necessary to it. We suggest this wording in the Draft Guidance be reconsidered.

(6.15) A disclosure to an unintended recipient will generally be a disclosure for a secondary purpose, even if the APP entity intended to disclose the personal information to a different recipient for the primary purpose of collection.

The Insurance Council is unclear as to why the Draft Guidelines consider a disclosure to an unintended recipient will generally be a disclosure for a secondary purpose. The Insurance Council submits the Draft Guidelines should be clarified to make it clear that a disclosure to an unintended recipient is an unauthorised disclosure (rather than a disclosure for a secondary purpose), or to provide the rationale for this statement.

(6.18) Consent is defined in s 6(1) as 'express consent or implied consent' and is discussed generally in Chapter B (Key concepts). The four key elements of consent are:

- ***it must be provided voluntarily***
- ***the individual must be adequately informed***
- ***it must be current and specific, and***
- ***the individual must have the capacity to understand and communicate their consent.***

The Draft Guidelines refer to express consent and implied consent as each requiring the above four elements. These four elements are problematic in relation to the concept of implied consent. For example how would entities:

- ascertain whether implied consent is current and specific and
- obtain communication of implied consent?

The Insurance Council submits the guidance is therefore contradictory and must be clarified so that the four elements apply only to express consent. We note this wording also appears at 7.24 and 8.29. We also consider that an annual renewal process which asks individuals to check the currency of their details should suffice.

Chapter 7 - APP 7: direct marketing

As a general issue, the Insurance Council considers the Draft Guidelines should not use examples that refer to email, SMS and calls (for example, at 7.30) as the *Spam Act 2003* and *Do Not Call Register Act* 2006 govern these communications. To avoid confusion, we suggest the Draft Guidelines do not provide examples in relation to communications dealt with specifically by other legislation.

Some parts of the Draft Guidelines relating to online advertising (for example 7.9 & 7.11) are also confusing. 7.11 provides as an example of direct marketing:

> ***'displaying an advertisement on a social media site that an individual is logged into, using personal information, including data stored on cookies relating to websites the individual has viewed'***

The Insurance Council submits this example should be clarified to ensure that advertisements shown to individuals in line with other websites they have visited (information logged in a cookie), without any individualised message tailored to the individual, would not be classed as direct marketing.

The Draft Guidance does not take into account a practical consideration of how to include an opt-out statement on online advertisements (for example, banners on websites or social media sites). Even if an advertisement included an op- out statement, the entity that places the online advertisement cannot opt the individual out of viewing such advertisements. Not all websites and social media services that host advertisements would give the user a means of turning off advertisements.

(7.18) The organisation should assess the reasonable expectations of the individual at the time of the proposed use or disclosure, rather than at the time that the personal information is collected.

We consider this example to be impractical and unnecessarily complex. The Draft Guidelines should be revised to make it clear that an entity is not required to revisit an individual's reasonable expectation whenever engaging in future direct marketing. The test should be an objective test and must recognise the individual's ability to opt-out, and the insurer's obligation to provide a prominent statement about the individual's ability to opt-out, of direct marketing.

(7.20) ***A simple means for opting out should include:***

- ***A clear and easily understood explanation of how to opt out, for example, instructions written in plain English and in a font size that is easy to read.***
- ***A process for opting out, which requires minimal time and effort***
- ***An opt out process that uses the same communication channel that the organisation used to deliver the direct marketing communication, for example, online or by post. An organisation could also provide additional opt out communication channels.***
- ***An opt out process that is free, or that does not involve more than a nominal cost for the individual, for example, the cost of a local phone call, text message or postage stamp.***

The Insurance Council is concerned the simple means for an individual to opt-out is being made unnecessarily complex. It should be sufficient that there is a simple means for an individual to opt-out, rather than requiring the same communication channel that the organisation used to deliver the direct marketing communication. In other words, an opt-out statement in a post mail-out which tells the individual to call a number to opt-out should be sufficient, rather than require opt-out by post. The Guidance should be clarified to make it clear an entity need not offer opt-out by the same method as the original communication.

7.24 repeats the four key elements of consent including that consent must be current and specific. In accordance with our previous comments, the Insurance Council submits that the Guidance must facilitate reliance on prior consent so it is clear that entities are not expected to contact individuals on each occasion they wish to undertake direct marketing. A requirement to contact, in some cases, many thousands of customers to revisit a prior consent would be impracticable, time-consuming and costly.

(7.25) Whether it is 'impracticable' for an organisation to obtain consent will depend on a number of factors, including the time and cost involved in seeking consent. However, it would not generally be considered impracticable to obtain consent due to the inconvenience or commercial cost of doing so.

The Insurance Council refers to its comments above at 7.24. In addition, we consider that the Guidance must acknowledge commercial costs as a legitimate factor to consider, together with other relevant factors.

(7.26) ***An organisation may obtain the consent from the individual in relation to a subsequent use or disclosure of the individual's personal information for the purpose of direct marketing at the time it collects the personal information. In order to rely on this consent, the organisation must be satisfied that it is still current at the time of the use or disclosure.***

We refer to our comments at 7.24 above.

(7.29) In addition, APP 7.3 requires an APP entity to provide a prominent statement that the individual may request to opt out in each direct marketing communication. This statement should meet the following criteria:

- ***The statement should be written in plain English, and not use legal or industry jargon.***
- ***It should be positioned prominently, and not hidden amongst other text. Headings may be necessary to draw attention to the statement.***
- ***It should be published in a font size and type which is easy to read, and at least the same font size as the main body of text in the communication.***

The Insurance Council considers it is unnecessary for the Guidance to require that the main body of text and opt-out statement appear in the same font size. It is submitted that differentiation of the opt-out statement may be beneficial and consistent with other types of communications individuals are familiar with. We submit therefore that the Draft Guidance should instead reflect the wording at 7.20: that the opt-out be in a font size that is easy to read.

7.39 An individual may also ask the organisation to identify the source of the personal information (APP 7.6(e)). The organisation must then notify the individual of its source, unless this is impracticable or unreasonable. Whether it is impracticable or unreasonable to notify the individual of the source of the personal information will depend on a number of factors, including:

- ***the consequences for the individual if they are not notified of the source***
- ***the length of time that has elapsed since the personal information was collected by the organisation***
- ***the time and cost involved. However it would not generally be considered impracticable or unreasonable to notify the individual of its source simply due to inconvenience or commercial cost of doing so.***

It is submitted that the Guidelines should take into account the impracticality for entities to identify some individual sources of historical information, for example where the request relates to information sourced many years ago and/or is derived from a combination of sources. The Insurance Council reiterates that time and cost involved should be given appropriate weight, along with other relevant factors, and not readily discounted within the Guidance.

Chapter 8 - APP 8: cross-border disclosure of personal information

(8.12) ***However, in limited circumstances, providing personal information to an overseas contractor to perform services on behalf of an APP entity may be a 'use'. ... For example, where an APP entity provides personal information to a cloud service provider located overseas for the limited purpose of storing and managing personal information, and:***

- ***the contract between the entity and the overseas cloud service provider binds the provider not to use or disclose the personal information except for the limited purpose of storing and managing the information***
- ***the contract requires any sub-contractors to agree to the same obligations, and***
- ***the contract between the entity and the cloud service provider gives the entity effective control of the information.***

The 'and:' at the end of the opening paragraph suggests the dot points are an exhaustive list of things that need to be checked positive for a provision of information to be classed as a 'use'. Paragraph 8.12 should be clarified that the contract provisions may assist with determining whether the arrangement is a 'use' or 'disclosure'. However, it should not be expected that contracts must or should contain all these provisions to make the provision of information a 'use'. Each case should be judged on its own facts.

Chapter 9 - APP 9: adoption, use or disclosure of government related identifiers
The Insurance Council makes no comments on this Chapter.

Chapter 10 - APP 10: quality of personal information
The Insurance Council reiterates concerns that some parts of the Draft Guidelines are unnecessarily complex , onerous and extend beyond what the APPs require (for example 6.12, 7.11, 7.18, 7.25, 10.12) and 10.19:

(10.19) To help an entity determine whether personal information from a particular point 10.19 in time is up-to-date for a particular purpose, records should clearly show the point in time to which the personal information relates.

This requirement appears unnecessarily onerous, as insurers may have multiple contacts with an insured during the course of a claim. It may also unnecessarily complicate current record management systems if, for instance, an updated address or contact phone number must also show a point in time to which the personal information relates. This may lead to unnecessary retention of old records to show the points in time information was received. We submit the Draft Guidelines should be amended so that it is not a blanket rule to require point in time information and that it only be required where it is reasonable and practical to do so.

Chapter 11 - APP 11: security of personal information
The Draft Guidelines at 11.5 provides that commercial cost or inconvenience is not a reason not to adopt appropriate information management. However, it must be recognised that some of the suggested actions require entities to go to great lengths to find and destroy all copies of the information which could be very costly:

- to destroy or de-identify information held in electronic form on a third party's hardware even though the organisation does not physically possess the information (11.23);
- if hardware cannot be sanitised, take steps to irretrievably destroy the information or putting it beyond use (11.28);
- where an organisation has instructed the third party to delete information, reasonable steps would include taking steps to verify that deletion has occurred (11.28);
- take reasonable steps to destroy or de-identify all copies of information held, including copies that have been archived or held as back-ups (11.24).

As previously submitted, we consider the Draft Guidelines do not adequately recognise the costs and practicalities for some entities which receive large volumes of information nor have sufficient regard to legacy systems and outsourcing arrangements. There are also legitimate legal reasons an entity may need to retain information, for example possible legal proceedings.