INSURANCE COUNCIL OF AUSTRALIA

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

By email: consultation@oaic.gov.au

20 September 2013

Dear Commissioner

DRAFT AUSTRALIAN PRIVACY PRINCIPLES GUIDELINES

The Insurance Council of Australia[1] (Insurance Council) appreciates the opportunity to provide comments on the first tranche of the draft guidelines (Draft Guidelines) for the Australian Privacy Principles (APPs).

We recognise that the concepts within the APPs are not dissimilar from the principles general insurers have been following for a number of years. However, Insurance Council members have identified some areas of the Draft Guidelines which would benefit from revision or clarification and others where additional guidance would be useful.

The **Attachment** provides comments aimed to ensure the Guidelines are sufficiently flexible for entities to comply with and that they facilitate the application of the APPs to the specifics of the general insurance industry.

The Insurance Council is concerned that in places the Draft Guidelines appear to discount cost as a relevant consideration of what is reasonable or practicable (for example, 5.4 and 2.21). We submit that cost should be a relevant factor, amongst of course others, and the Guidelines should appropriately reflect this. Costs can have a direct affect not only on the entity but on consumers as they may not be able to be absorbed by the business.

---

[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

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

This attachment details the issues raised by Insurance Council members in relation to the Draft Guidelines.

CHAPTER B: KEY CONCEPTS

(B.11 and B.12) 'Carries on business in Australia'

The Insurance Council would appreciate the Guidelines providing information on whether an entity located overseas (legally separate to an Australian insurer within the same group) which offers a mobile software application able to be downloaded in Australia but is otherwise not offering an insurance or other products or services to individuals in Australia over the internet or by other means, is likely to be considered 'carrying on business' for the purposes of s 5B(3)(b) of the Privacy Act?

(B.36) Consent: current and specific.

The Insurance Council has concerns about the implications of B.36 in the general insurance context. The Draft Guidelines state that an individual may withdraw their consent at any time. If they do, an APP entity would no longer be able to rely on consent having been given when dealing with the individual's personal information.

Our members require certainty that legitimate uses flowing from the original provision of consent for collection, use or disclosure can be maintained. Insurers otherwise may be placed in an untenable position where they have a continuing contractual obligation under a policy but are deprived of the use of necessary information obtained with the consent of the insured. Withdrawal of consent may lead to the insurer needing to cancel the policy.

In addition, the insured has a duty of disclosure under the Insurance Contracts Act 1984. It is unclear what the impact this provision in the guidelines would have on information collected in fulfilment of this duty as there is no provision in the Act allowing the disclosure to be withdrawn. It may prevent the insurer from entering into the contract or, if the contract is already on foot, prevent for example, the processing of a claim. It seems illogical from both a practical and contractual perspective that one party to a contract can provide consent to the use of information necessary for implementation of the contract but later withdraw it entirely. We query whether this is the intention of the Draft Guidelines.

The Insurance Council submits the Draft Guidelines should make it clear that allowable uses made pursuant to the original provision of consent cannot be undone by the subsequent withdrawal of consent.

AUSTRALIAN PRIVACY PRINCIPLES GUIDELINES

Chapter 1, APP 1: open and transparent management of personal information

(1.9) The policy is also not required to contain the same level of detail as a collection notice provided to an individual under APP 5.1, which will provide more specific information relevant to a particular collection of personal information from the individual.

Although not explicit, 1.9 (and see also 5.1 – 5.3) seems to suggest that the privacy policy and collection notice may not be contained in one document and provided simultaneously.

However, the APPs do not appear to preclude specifically the provision of the privacy policy and collection notice at the same time. Consequently, our members believe the Guidelines should explicitly allow the option for an entity to provide both in one document. In the case of general insurance, this would provide efficiencies for both the insurer and insured (ease of reference), as there is likely to be a large overlap of information between the two. This will also assist to simplify web based transactions by limiting the number of pop-up boxes that an individual must read.

It must be borne in mind that at the beginning of an insurance transaction (i.e. when a customer takes out a policy) an insurer is legally required to provide a customer with extensive information. The customer is:

- asked a series of underwriting questions;
- often provided a duty of disclosure notice;
- provided a verbal Product Disclosure Statement (PDS) notice if a retail client (if the transaction is over the phone) with a Certificate of Insurance and PDS and Policy Booklet to follow in the mail;
- provided a Certificate of Insurance and a PDS and Policy booklet if a retail client (if the transaction is in person or often when web based);
- provided a statement of advice if a retail client (if personal advice is given as part of the transaction); and
- provided a financial services guide in certain circumstances

All of this can induce information overload in a customer. This would be exacerbated if the insurer had to provide a collection statement (which deals with APP5) and in addition refer the customer to a Privacy Policy to read.

Furthermore, in many instances a customer will purchase insurance through an intermediary meaning that the insurer does not interact with the customer directly. Rather, an intermediary will be relied upon to convey privacy matters to the customer until such time as the insurer can distribute documentation to the customer shortly after the transaction takes place. The intermediary may well have its own collection statement to convey. By having the insurer's collection statement within its privacy policy, the insurer can be confident that the desired information is passed on to a customer accurately and in appropriate language,

The Draft Guidelines make clear that an APP entity's privacy policies should, inter alia, be easy to navigate, clearly expressed, and readable by a diverse community. We believe that the option of allowing a privacy policy, where practicable, to be a single source of privacy information makes these goals easier to achieve to the benefit of consumers and APP entities alike.

(1.25 – 1.27) Likely overseas disclosures

The Insurance Council would appreciate revision of these sections.

A list of the countries where disclosure may be likely is to be included, if practicable in a privacy policy. The Draft Guidelines note that although the Act does not specify when it will be considered impracticable to provide such as list, a possible example is where there are numerous overseas recipients and determining where those recipients are likely to be located is unduly costly. However, the Draft Guidelines suggest that in such as case, 'the more practical option may be to list those countries in an appendix to the APP Privacy

Policy". This seems to be contradictory and we would question what purpose a lengthy list of possible countries would serve from a customer's point of view.

Furthermore, 1.25 states:

"The policy should note the kinds of personal information that are likely to be sent to particular countries."

This requirement goes beyond what the APPs require and the Insurance Council requests that this requirement be removed from Draft Guidelines.

Chapter 2, APP 2: anonymity and pseudonymity

(2.13) The steps an APP entity should take to draw both options to the attention of individuals will depend on the nature of the dealing between the entity and an individual. At a minimum, an entity's APP Privacy Policy (APP1) should explain the circumstances in which an individual may deal anonymously or by pseudonym with the entity, and the procedures for doing so. The APP Privacy Policy may need to go further and explain how the entity manages pseudonyms and any linked personal information, and if an individual will be placed at a disadvantage by dealing anonymously or through a pseudonym (for example, where only a limited service can be provided). In summary, often more than a simple statement in an APP Privacy Policy that individuals can deal anonymously or by pseudonym with the entity will be required.

The above requirements in the Draft Guidelines go beyond what the APP 2 requires. There is no suggestion in APP2 that the Privacy Policy should contain this information. The Insurance Council requests that this paragraph be revised.

(2.21) In special circumstances it may be open to an entity to rely on the 'impracticability' exception where it would be unduly costly for the entity to provide a service to an unidentified individual or to change an existing system or practice to include the option of anonymous or pseudonymous dealings. However, this is more likely to be a transitional rather than an ongoing justification. All APP entities are expected to design and maintain information collection systems that incorporate anonymous and pseudonymous options.

Similar to above, this section appears to go beyond what the APPs require and the Insurance Council would like to see it revised. The ability to deal with customers in an anonymous or pseudonymous way is possible in only limited situations in general insurance, for example when factual information is first being sought about a policy or an inquiry is being made about a quote. However, in an ongoing contractual relationship requiring the utmost good faith on both sides, the real identity of the insured is needed. For example, when dealing with a specific claim, it is reasonable that the insured is properly identified.

The guidelines should therefore recognise explicitly that for some industries, such as general insurance, anonymous and pseudonymous options are not possible for many types of transactions.

Chapter 3: collection of solicited personal information

(3.7) Examples of solicited information include:

• information provided to a 'fraud hotline' that is designed to capture 'tip-offs' from the public

A number of Insurance Council members operate 'hotlines'. However, despite having a hotline service available, individuals may instead make contact with an insurer through other means such as by anonymous email or mail. This information would need to be treated as unsolicited when it is not substantially different to the information "solicited" via the fraud hotline.

The Insurance Council submits that it would be reasonable to treat all information provided on fraud as 'solicited'. This would be on the basis that the insurer in general invites fraud tip-offs. There would need to be acknowledgement that it would be reasonable in such situations not to provide a privacy notification (under APP 5) because for example, the identity of the person providing the information is unknown or to avoid alert the potential fraudster that they are being investigated.

Chapter 4: dealing with unsolicited information

(4.11; 4.26; 4.27):

> ***What is a 'reasonable period' for deciding whether unsolicited personal information could have been collected under APP 3 will depend on the circumstances of the particular case. The entity should decide that issue promptly after the unsolicited information is received.***
>
> ***The requirement that unsolicited personal information be destroyed or de-identified 'as soon as practicable' requires prompt action by an organisation. That is, an organisation should promptly identify that it has collected unsolicited personal information, that the information could not be collected under APP 3, and that it would be lawful and reasonable to destroy or de-identify it. Prompt action should then be taken to destroy or de-identify the information.***
>
> ***In adopting a timetable that is 'practicable', an organisation can take technical and resource considerations into account. However, those considerations must be balanced with the organisation's obligation to act promptly when required by APP 4.3 to destroy or de-identify unsolicited personal information.***

The Insurance Council is concerned that the Draft Guidelines equate the term 'prompt' with the phrases 'reasonable period' and 'as soon as practicable'. We consider this term represents a higher standard than that required by the APPs and has the likelihood of being problematic for general insurers which receive a large quantity of unsolicited information from a variety of sources.

Reasonable time is necessary for entities to properly consider the range of information received. For example, an insurer may receive police reports containing information from and about several witnesses yet may not be in a position to know whether the information is needed until sometime in the future.

Chapter 5: notification of the collection of personal information

State mandated insurance

The Insurance Council would appreciate the Guidelines addressing the issues faced by a number of our members which provide insurance such as Workers' Compensation or

Compulsory Third Party Motor Vehicle in line with State Government requirements. While these insurances are mandated by State Governments, our members are the insurers under the policies issued by our members (as opposed to the State being the insurer). In these cases, the documentation is closely specified by the State Government and has a set privacy notice which the insurer cannot vary. The insurer should not be required to also provide its own privacy notice. An additional privacy notice would not lead to better protection of personal information but only increase costs.

Similarly, with some State Government mandated schemes, the insurer collects the policyholder's information from the relevant Government authority and not directly from the individual. It would appear reasonable in these situations that the only privacy notice required is issued by the Government Authority.

(5.5) The following are given as examples of reasonable steps that an APP entity could consider:

- ***if personal information is collected by telephone – explaining the APP 5 matters to the individual at the commencement of the call (perhaps following a template script)***
- ***the individual should be asked to confirm they have reviewed the notice before providing their personal information.***

It would be helpful if the Guidelines indicated that it is reasonable for entities to provide an option at the beginning of a telephone call allowing customers to elect to listen to a privacy notice (whether in full or short form). An alternative would be a short Interactive Voice Response (IVR) notice to be heard prior to the transaction which refers the customer to a privacy notice which can be reviewed on the entity's website or sent to the customer on request.

This would address a number of issues including:

- the practicalities for a customer who may have time limitations and is seeking to quickly obtain a quote or endorsement to a policy;
- it may unnecessarily irritate a customer who is already aware of privacy matters to be referred automatically to a lengthy template script; and
- minimisation of unnecessary costs for the insurer flowing from having to read a script which the consumer does not want to hear.

Under the Corporations Act 2001 and the Insurance Contract Act 1984, provision is made for notices to be flexible which enables insurers not to provide customers too much information at once and for transactions to be efficient[2]. It would be appropriate for the Guidelines to do the same

The Insurance Council queries the provision in the Draft Guidelines that an individual should confirm they have reviewed a notice. It should be a matter for the individual alone whether they have reviewed a notice. It is recommended this requirement be removed from the Guidelines. It is not a requirement under the APPs and may be impractical in certain situations.

[2] For example, see section 69 of the Insurance Contracts Act 1984 and section 1012G of the Corporations Act 2001.

(5.6) When not taking any steps may be reasonable

Our members are concerned that bullet point two suggests a specific notice, tailored to each collection may be required unless under 5.6:

- ***an entity collects personal information from an individual on a recurring basis over a short period in relation to the same matter, and the individual is aware (or reasonably ought to be aware) that a separate notice will not be issued for each instance of collection***

This would be problematic. The Draft Guidelines raise issues about what is to be considered the 'same matter' and what is a 'short period' and the possibility of having to give multiple notices to the one person if a notice needs to be given every time personal information is collected from an individual. The Insurance Council recommends that the Guidelines be clarified to avoid unnecessary confusion for insureds in receiving multiple notices as well as the cost to the insurer of developing and delivering such notices.

It is submitted that one clear notice should be all that is required except in exceptional circumstance e.g. where collection required by an Australian law. It is likely the policy that the customer has with their insurer will contain provisions or reference to provisions dealing with APP 5 and therefore a customer who has a policy will be able to reference this document. Further, if information is available for example on an IVR that refers customers to a notice, then no further notice should be required.

In relation to the insurance policy itself, insurers will frequently provide annually renewing cover to the same customers over a number of years and we do not believe it would be practicable (nor advantageous to the customer) to continue to provide notice to those customers when policies are updated given the purpose for collection remains fundamentally the same.

We recommend therefore that the phrase "over a short period" be removed to recognise that recurring information collection within long-standing and familiar relationships do not warrant repeat notification.

Further, the Insurance Council would welcome the Guidelines highlighting some general insurance examples of situations where it is reasonable not to provide a privacy policy, such as:

- where the insurer is merely a co-insurer and personal information is collected through a lead insurer, underwriting agency or broker;
- where the insurer relies on agency law by providing an intermediary (such as a broker) with the privacy notice and the intermediary (acting as the agent of the insured) is to provide the notice directly to the insured.

(5.8) The APP entity's identity and contact details

The Draft Guidelines set out that 'contact details' should include the position title, telephone number and email address of a contact who handles enquiries and requests relating to the Privacy Act. This requirement also appears at 1.21.

We note the Draft Guidelines suggest consideration be given to establishing a generic telephone number and email address that will not change with staff movements. However,

the Insurance Council is concerned that this is not practicable, particularly for large entities which may have a numbers of sections dealing with privacy matters for particular parts of the organisation.

It should also be recognised that position titles change from time to time. We suggest the Guidelines be revised to simply require the contact details which will enable the person to speak to someone in the organisation about a privacy issue. Furthermore, in relation to 5.8 we note that AAP5.2(a) does not require notification of the "position title, telephone number and email address of a contact who handles enquires and requests relating to the Privacy Act". It only requires notification of "the identity and contact details of the APP entity."

(5.9) The facts and circumstances of collection

The Draft Guidelines state that a notice is to include the circumstances of the collection, such as the date, time, place and method. Our members are concerned this suggests a specific notice, tailored to each collection may be required unless bullet point two under 5.6 applies (see above).

With privacy notices in insurance documentation printed in bulk for distribution, it is not possible for them to be amended for each instance of collection to specify the date, time, place and method of collection before it is given to an individual. The guidance under 5.6 also raises issues about what is to be considered the 'same matter' and what is a 'short period'.

The Insurance Council recommends that the Guidelines be clarified to remove the requirement to state the date, time, place and method of collection to avoid unnecessary confusion for insureds in receiving multiple notices as well as the likely costs associated with such notices.

Our comments above in relation to 5.6 in relation to the concern we have about multiple notices are also relevant.

(5.11) Where personal information is collected from an entity other than an individual, the notice should include the name of that entity.

Our members collect information from a wide variety of sources. As mentioned above under 5.9, it would not be possible to amend privacy notices for each instance of collection as this would require listing all entities, such as service providers or witnesses. It would be realistic to require a general indication of the kinds of entities from which information is collected. The Guidelines would therefore benefit from recognition of the impracticalities that arise for certain entities to provide the names of all entities.