INSURANCE COUNCIL OF AUSTRALIA

4 December 2020

The Privacy Act Review
Attorney General's Department
Robert Garran Offices
3-5 National Circuit
**Barton ACT 2600**

**By Email**: PrivacyActReview@ag.gov.au

Dear Sir/Madam

## REVIEW OF THE PRIVACY ACT 1988 (CTH) ISSUES PAPER

The Insurance Council of Australia[1] ("Insurance Council"), welcomes the opportunity to provide a submission in response to the Attorney-General's Department Issues Paper for its review of the *Privacy Act 1988* (Cth).

As you would be aware, in the course of providing insurance and paying claims, it is necessary for insurers to collect, use, disclose and handle considerable amounts of personal information. The information ranges widely from names and addresses to sensitive health information. Insurance Council members understand and recognise the importance of privacy and the protections afforded to individuals under the privacy framework. Consequently, members take their privacy obligations very seriously and invest time and capital in systems, training and policies to promote a culture that respects and protects privacy.

The insurance industry relies heavily on access to a broad range of long-term, longitudinal data to identify, measure and price risk in providing cover to individuals and businesses. Some of this data is obtained from and held by a range of government entities. Foundational data concerning factors such asset location, population, topography and specific hazards (for example bushfire and flood) are critical to assessing risk accurately.

The utilisation of granular data allows both insurers and policyholders to improve their understanding of insurable risk and how to appropriately manage it. This enables the general insurance sector to design and tailor products which meet the individual needs of their customers. The Insurance Council acknowledges that the counterpart to the use of data to

[1] The Insurance Council of Australia is the representative body of the general insurance industry in Australia. Insurance Council members represent about 95 per cent 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.

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).

personalise products is an equitable balance between appropriate privacy protection and effective provision of insurance.

The general insurance industry is governed by an extensive framework of laws and regulations which governs financial services and promotes and protect consumers. This regime will be enhanced by legislation recently introduced into Parliament in response to the Financial Services Royal Commission. In addition, as you will be aware, a consumer data right commenced in the banking sector from 1 July 2020 and is expected to be extended to other industry sectors, including general insurance. Insufficient consideration of the issues specific to the financial services industry when revising the policy and legislative frameworks which govern privacy is likely to lead to confusion and inefficiencies for both consumers and industry.

As a condition of membership, Insurance Council members also adhere to the General Insurance Code of Practice. Following an extensive review, the general insurance industry is currently in the process of bringing to life its updated 2020 Code.[2] The 2020 Code includes provisions at Part 9 (*Supporting customers experiencing vulnerability*) and Part 10 (*Financial hardship*) to take extra care with vulnerable customers, so insurers can work with these customers to arrange additional support, including flexible options for those experiencing financial hardship. The code provisions in Parts 9 and 10 were fast-tracked during the COVID-19 pandemic and come into full effect on 1 January 2021.[3] The remaining Code provisions, including a new Part 12 (*Your access to your information*) will come into effect on 1 July 2021. As general insurers focus on supporting customers and inclusion, their preference is for any changes to the privacy framework to support, and not inhibit, their ability to provide appropriate responses to vulnerable customers.

To assist your understanding of how possible changes to the Privacy Act may impact general insurers, the views of Insurance Council members and their responses to the questions raised in the Issues Paper are set out in the Attachment. In due course, the Insurance Council would welcome the opportunity to discuss any proposed changes to the Privacy Act directly with the Attorney-General's Department.

If you have any questions or comments in relation to our submission, please contact Aparna Reddy, Senior Policy Advisor, Regulation Policy on (02) 9253 5176 or areddy@insurancecouncil.com.au

Yours sincerely

Andrew Hall
Executive Director & CEO

---

[2] 2020 General Insurance Code of Practice
[3] ICA Media Releases *Insurance Council fast-tracks new Code of Practice vulnerability and hardship provisions* (7 May 2020) and *Insurers boost support for customers experiencing family violence, financial hardship and vulnerability* (1 July 2020)

INSURANCE COUNCIL OF AUSTRALIA

**ATTACHMENT**

## INSURANCE CONCIL RESPONSE TO REVIEW OF THE PRIVACY ACT 1988 (CTH) ISSUES PAPER

### *Objects of the Privacy Act*

1. Should the objects outlined in 2A of the Act be changed? If so, what changes should be made and why?

Insurance Council members are comfortable with the current objects outlined in section 2A of the Privacy Act. These recognise that the protection of the privacy of individuals needs to be balanced with the ability for businesses to carry on their legitimate activities. Members are bound by the Australian Privacy Principles (APPs) and take active steps to ensure compliance and recognise their importance in upholding robust privacy protections for consumers.

### *Definition of personal information*

4. Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?
5. Are any other changes required to the Act to provide greater clarity around what information is 'personal information'?

Insurance Council members would caution against additional regulation of de-identified, anonymised and pseudonymised information. Broadly, under APP 2, customers have the option of not identifying themselves or using a pseudonym but it will generally be impracticable for insurers to provide their services or products to customers unless they are able to gather essentially personal information to ascertain and price for risk.

Our members would also caution against broadening of what constitutes 'personal information'. Sound general insurance practice has always relied on public and private data in identifying and measuring risk. If a broadening of what constitutes 'personal information' results in less data being available for public use, this potentially limits the opportunities for insurers being able to draw on emerging data and trends to price for risk, undertake product innovation, engage with consumers and manage claims.

### *Flexibility of the APPs in regulating and protecting privacy*

6. Is the framework of the Act effective in providing flexibility to cater for a wide variety of entities, acts and practices, while ensuring sufficient clarity about protections and obligations?

Insurance Council members consider the current privacy framework to be satisfactory. Any potential amendments to the privacy framework should be considered within the context of the existing principles-based approach. As noted above, this approach balances privacy protections with the ability of businesses to conduct their operations and service the needs of

the community. Any changes being considered should be evaluated against the goal of making it easier for individuals to engage efficiently with businesses while having their personal information appropriately protected.

Insurance Council members note that a principles-based approach requires regulatory guidance to set out community expectations on key issues.

***Notice of Collection of Personal Information***

20. Does notice help people to understand and manage their personal information?
21. What matters should be considered to balance providing adequate information to individuals and minimising any regulatory burden?
22. What sort of requirements should be put in place to ensure that notification is accessible; can be easily understood; and informs an individual of all relevant uses and disclosures?
23. Where an entity collects an individual's personal information and is unable to notify the individual of the collection, should additional requirements or limitations be placed on the use or disclosure of that information?
24. What measures could be used to ensure individuals received adequate notice without being subject to information overload?
25. Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are used their personal information?

Insurance Council members are concerned about the implications of introducing a requirement for an express notice to be given when collecting personal information. Information collection by insurers is limited to that provided by a consumer expressly so that insurers may deliver products or services to them. The purpose of information collection in insurance is not for large scale aggregation purposes by advertisers. The current framework allows insurers to collect, use and disclose information where it is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.

Insurance Council members believe that there are already a number of appropriate, written notifications to consumers when collecting information to provide insurance products. Introduction of a specific 'notice of collection' may have the opposite impact intended. Given that consumers already receive many disclosures and notices regarding insurance, providing additional ones may result in confusion and/or refusal to properly read and understand the information supplied.

In response to Question 23, it would be impractical for insurers to always notify particular third parties, such as witnesses of motor vehicle claims, that their personal information may be needed and collected via the policyholder. In fact, Insurance Council members submit that not only should the information be able to be used to establish, exercise or defend a legal or equitable claims, this right may need to be strengthened to make it clear that the information can also be used to obtain legal advice about the event.

INSURANCE COUNCIL OF AUSTRALIA

***Consent to collection, use and disclosure of personal information***

27. What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?
28. Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consents for each primary purpose?
32. Should entities collecting, using and disclosing personal information be required to implement pro-privacy defaults for certain uses and disclosures of personal information?

Insurance Council members submit that the existing framework for privacy protection appropriately requires the provision of notice to consumers to collect, use and disclose their personal information when providing general insurance products. In addition, Insurance Council members provide straightforward, plain English privacy statements/policies either on request or through websites. Consequently, proposals that would require additional consent or written notice before collection, use or disclosure of personal information need careful consideration of sector specific issues, and how they may interact with industry specific regulatory frameworks.

In the absence of clear consumer benefit, it would be impractical and inefficient to require additional, especially written, consent for the collection of consumer's personal information for the provision of general insurance products. Below are some scenarios which detail how a notification requirement may hinder the provision of general insurance products:

- A written notification requirement would limit the ability for insurers to provide quotes to prospective customers who contact general insurers by telephone, as written notice would first need to be provided prior to information collection. This would delay the provision of the quote, and potentially insurance cover in time-critical situations.
- The diversity of products and services provided by insurers (including natural disaster assistance, risk management and education) would make it likely that a broad collection notice would be required, in order to avoid new notices having to be provided at different stages of claims management process. This would be of minimal benefit to consumers.
- Insurers would need to carefully consider each contact with a consumer involving collection of information as to whether what is being collected is covered by an existing collection notice, potentially slowing down the processing of claims against insurance policies.
- New collection notices may be required when insurers engage third-party service providers to assist in the claims management process, which would be frustrating and inefficient.

One approach may be a prescribed list, where opt-in written consent is only required where the collection would be around 'exploitation' of personal information, for example sale of data to third parties, unrelated to the provision of goods or services requested by the consumer. This approach would also be relevant to question 32, such that a customer's personal

information should be protected, not exploited, nor used for a purpose other than for the purpose it was provided.

***Consent to collection and use and disclosure of personal information – emergency declarations and regulating use and disclosure***

41. Is an emergency declaration appropriately framed to facilitating the sharing of information in response to an emergency or disaster and protect the privacy of individuals?
42. Should reforms be considered to restrict uses and disclosures of personal information? If so, how should any reforms be balanced to ensure that they do not have an undue impact on the legitimate uses of personal information by entities?

As explained in the Insurance Council's submission[4] to the Royal Commission into National Natural Disaster Arrangements (RCNDA), an important operational learning from the Black Summer Fires is that there needs to be greater sharing and coordination of data by and from State Governments. In the Insurance Council's experience, each State Government collects impact assessment data following disasters. However, due to privacy concerns, State Governments frequently refrain from making that data available to insurers.

There is a significant community benefit in providing impact assessment data to insurers as it allows for funds and other benefits (such as emergency accommodation) to be made available to residents without the insurer having to wait until the property is accessible (which can take many weeks if a disaster is prolonged).

The Insurance Council recommended in its submission to the RCNDA that the Commonwealth and State Governments establish an effective data sharing framework. This would involve work with the Office of the Australian Information Commissioner (**OAIC**) and other relevant stakeholders such as the Insurance Council, to identify and remove impediments in the Privacy Act to the development of an effective data sharing framework .

The RCNDA Report[5] recommendations 4.6 and 4.7 support consistent impact data standards across State and Territory Governments as well as the development of greater capacity to collect and share standardised and comprehensive natural disaster impact data.

The Commonwealth Government's response to the RCNDA[6] supported recommendations 4.6 and 4.7, noting the State and Territory Government responsibilities in the area. The Commonwealth Government noted that its commitment to establish 'Resilience Services' by 1 July 2021, a climate and disaster risk information service, as an important step towards achieving a greater capacity to collect and share standardised and comprehensive natural disaster impact data.

[4] Insurance Council of Australia – Submission to the Royal Commission into National Natural Disaster Arrangements – 28 April 2020.
[5] Final Report – Royal Commission into National Natural Disaster Arrangements – 28 October 2020
[6] A national approach to national disasters – The Commonwealth Government's response to the Royal Commission into National Natural Disaster Arrangements – November 2020

The RCNDA Report also supported Australian, State and Territory Governments considering the extent to which de-identified personal information provided by affected persons can or should be included or connected with impact data to facilitate timely recovery support.

The Insurance Council would welcome the opportunity to work with all levels of government to progress recommendations 4.6 and 4.7 together with consideration of removing any impediments to provision of impact assessment data to insurers.

***Control and security of personal information, right to erasure***

43. Are the security requirements under the Act reasonable and appropriate to protect the personal information of individuals?
44. Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?
46. Should a 'right to erasure' be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities?
47. What conditions are necessary to achieve greater consumer control through a 'right to erasure' without negatively impacting other public interests?

Insurance Council members are concerned over the implications of introducing a blanket 'right to erasure' in respect of key insurance data. Whilst members are supportive of the ability for a consumer to require erasure of personal information from a digital platform not associated with the provision of insurance products, they believe any extension of this right to information held by insurers would affect their ability to respond to claims, complaints and/or investigations. This would particularly be the case in circumstances which can sometimes arise years after an initial claim. This information is also critical to comply with reinsurance treaty obligations and regulatory requirements.

Reinsurance is a key component in assisting Insurance Council members managing risk. Under their reinsurance agreements, insurers provide data used for broader claim analysis. If a 'right to erasure' of personal of information was exercised, our members are concerned that information within this analysis would then need to be extracted, or de-identified.

Insurance Council members are also subject to data reporting requirements from regulators, including the Australian Prudential Regulation Authority, the Australian Securities and Investments Commission and the Australian Financial Complaints Authority. Any such right to erasure should not operate contrary to our members' regulatory obligations.

To accommodate the provision of general insurance services and products and meet the industry's reporting obligations to regulators, one possible approach may be to allow consumers to opt-out of a right to erasure with express consent of the insured, for example, as part of an insurance contract.

***Enforcement powers under the Privacy Act and the role of the OAIC and direct of action***

53. Is the enforcement framework for interferences with privacy working effectively?
54. Does the current framework approach achieve the right balance between conciliating complaints, investigating systematic issues, and taking punitive action for serious non-compliance?
55. Are the remedies available to the Commissioner sufficient or do the enforcement mechanisms available to the Commissioner require expansion? If so, what should these enforcement mechanisms look like?
56. How should any direct right of action under the Act be framed so as to give individuals greater control over their personal information and provide additional incentive for APP entities to comply with their obligations while balancing the need to appropriately direct court resources?

Insurance Council members supports the role of the OAIC and endorse the investigative and enforcement powers necessary for it to fulfill its functions.

Insurance Council members note that the ACCC in its Digital Platforms Inquiry report extensively canvassed the enforcement and regulatory agencies with responsibility for the Privacy Act and supported adequate resourcing of the OAIC to support its functions. ICA members agree that the OAIC should be resourced to utilise its existing powers more actively.

In addition, members consider that it would promote the protection of privacy if the OAIC were to take on a more active role in the early resolution stage of its complaint resolution process. This would provide an opportunity for individuals to gain a deeper understanding of how the Privacy Act and the APPs apply. This would also help parties to identify if, in the first instance, an interference may have occurred before trying to conciliate the complaint through OAIC.

***Statutory tort***

57. Is a statutory tort for invasions of privacy needed?
58. Should serious invasions of privacy be addressed through the criminal law or through a statutory tort?
59. What types of invasions of privacy should be covered by a statutory tort?
60. Should a statutory tort of privacy apply only to intentional, reckless invasions of privacy or should it also apply to breaches of privacy as a result of negligence or gross negligence?
61. How should a statutory tort for serious invasions of privacy be balanced with competing public interests?
62. If a statutory tort for the invasion of privacy was not enacted, what other changes could be made to existing laws to provide redress for serious invasions of privacy?

Insurance Council members caution against a new statutory tort for invasions of privacy. A tort has the potential to increase the risk of exposure of policy holders to public liability claims in particular. Insurers would need to reflect the greater risk they were taking on, by either specifically excluding the tort from coverage or re-evaluating the price of insurance products.

If a statutory tort is introduced, it should be confined to intentional or reckless invasions of privacy. A reasonably high threshold needs to be established to determine whether behaviour is intentional or reckless, to discourage frivolous or vexatious claims. The statutory tort does not need to extend to negligent claims, as these are already appropriately regulated under the current Privacy Act, with suitable mechanisms for handling complaints, redress and penalties.

Insurance Council members strongly believe that any statutory tort would need accompanying guidance on factors that courts may consider in determining whether a person in the position of the plaintiff would have a reasonable expectation of privacy. There needs to be clarification on the overlap between privacy invasions (under the proposed tort) and information privacy breaches (under the Privacy Act) are treated as well as the treatment of exemptions in Part II Division 3 of the Privacy Act.

Concerns also extend to the possibility of those seeking redress in multiple forums, including alternative dispute resolution (ADR) through the OAIC or the Australian Financial Complaints Authority (AFCA). There should a clear rationale as to why plaintiffs should be allowed to seek redress under more than one avenue. Otherwise defendants would potentially have completed a prescribed complaint process and still have to defend an action in tort.

***Interaction between the Act and other regulatory schemes***

66. Should there continue to be separate privacy protections to address specific privacy risks and concerns?
67. Is there a need for greater harmonisation of privacy protections under Commonwealth law? If so, is this need specific to certain types of personal information?
68. Are the compliance obligations in certain sectors proportionate and appropriate to public expectations?

Insurance Council members note that there are existing and adequate avenues for privacy related complaints against insurers. This is either through the AFCA and more broadly under section 52 of the Privacy Act which allows for privacy determinations by the OAIC.

AFCA is recognised as an external dispute resolution scheme under the Privacy Act so that AFCA may consider privacy disputes in relation to handling of personal financial or credit-related information with anything outside of that jurisdiction to be referred to OAIC. However, Insurance Council member feedback is that it has not precluded matters from being heard at both AFCA and the OAIC, either at the same time, or one after another on the same complaint. This appears to be highly dependent on the case officer in question at either the OAIC or AFCA. This potentially leads to double handling and extra compliance burden.