Insurance Council of Australia

Submitted via online portal:

https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/intro/

24 January 2022

To whom it may concern

Review of the Privacy Act 1988: Discussion Paper

The Insurance Council of Australia (Insurance Council) welcomes the opportunity from the Attorney-General's Department (AGD) to comment on the Discussion Paper, *Review of the Privacy Act 1988*.

The Insurance Council is the representative body of the general insurance industry in Australia and represents approximately 95 percent of private sector general insurers. As a foundational component of the Australian economy the general insurance industry employs approximately 60,000 people, generates gross written premium of $57.4 billion per annum and on average pays out $164.2 million in claims each working day ($42.7 billion per year).

Overview

The Insurance Council thanks the AGD for consultation paper and workshops. Below, the Insurance Council has provided more detailed responses to select questions that are of particular impact to our members. At the outset, it is worthwhile outlining several of the common themes that run through our response.

Most importantly, any changes to the *Privacy Act 1988* will need to be implemented across the economy and therefore will have economy-wide impacts. They will need to be realistically implementable across a range of businesses. The *Privacy Act* currently addresses this by adopting a principles-based approach. The legislation sets key outcomes and allows businesses to meet those outcomes in a manner that aligns with their economic situation, industry practices and business needs. As this is a technologically neutral approach, it has the advantage of providing for flexibility in accommodating emerging technologies and supporting development of innovative products.

The Insurance Council suggests that the current proposals would move away from a principles-based approach and towards a more prescriptive model. Several examples of this are outlined in our response below. For example, the right to erasure is potentially complicated by generational differences of systems between different businesses. Some insurers have customer documentation and records dating back several decades (given claims may still arise under insurance cover taken out many years ago), which may not be digitised. Such changes will likely pressure businesses with large amounts of legacy systems in place, while favouring greenfield start-ups. The cost of change for existing service providers may be high.

Insurance Council of Australia

A corollary to this point is that the "problem statement" for some proposals is often not evident. In some cases, it appears that the underlying issue would likely be solved by specific guidance from the Office of the Australian Information Commissioner (OAIC). For example, for some proposals, it is unclear whether the underlying concern relates to ***first-party*** or ***third-party*** use of data. In several cases, while it appears that the underlying concern relates to ***third-party*** use of data, the proposals would also impact ***first-party*** use of data. In these cases, the Insurance Council suggests that a more tightly defined problem would help clarify the need for new rules and their scope.

Based on the above, the Insurance Council **recommends** that greater consideration be given to the real-world impact of the proposals. This would involve testing the proposals in a range of real-life scenarios and would support a customer-centred approach. It would also involve testing proposals to ensure that they appropriately aligned with existing industry best practice. For example, this could include testing any new notification or consent requirements against existing disclosure requirements. While consumer testing has been proposed for some proposals (eg. notification requirements), the Insurance Council suggests that it may need to be broader. The Insurance Council would welcome the opportunity to assist the AGD on these matters.

Finally, it is worth reinforcing the point that effective use of consumer data is critical to both the insurance industry and the economy as a whole. The Australian Government's whole-of-economy vision statement, the *Australian Data Strategy*, recognises the significant and growing role that data plays in the economy:[1]

- *Data is a valuable national asset that, when leveraged effectively, can bring transformative benefits to its users and to individuals and the economy more broadly.*

Further noting that:

- *The private sector also has a long history of using data to benefit its clients through better and more tailored services and offerings.*

Within the insurance industry, data is a crucial input to identifying, measuring and pricing risk and paying claims made by customers. Data is used in all facets of the insurance product life cycle – including product design, underwriting and claims handling. Insurers use both non-personal datasets (for example, data on natural hazards) as well as personal data provided by customers. A 2017 report by McKinsey identified several uses of data analytics in enhancing the customer experience.[2] These include – enhancing existing business models, strengthening channel relationships with consumers, changing relationships with consumers (for example, use of telematics to offer usage-based policies), re-designing products and establishing adjacent businesses. Any proposed changes to privacy regulation will need to consider real-world impacts and should be tailored in such a way as to effectively address clearly identified problem statements.

[1] Department of the Prime Minister and Cabinet, *Australian Data Strategy: The Australian Government's Whole-of-Economy Vision for Data* (link), page 5
[2] McKinsey Consulting, *Harnessing the Potential of Data in Insurance*, (link)

Insurance Council of Australia

Proposal 1: Objects of the Act

1.1 Amend the objects in section 2A, to clarify the Act's scope and introduce the concept of public interest, as follows:
(a) to promote the protection of the privacy of individuals with regard to their personal information, and
(b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities undertaken in the public interest.

Proposal 1.1 would, among other things, amend the Objects of the *Privacy Act* to provide that "the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities ***"undertaken in the public interest"*** (emphasis added). The Proposals paper (page 19) describes this as a "balancing exercise" that is guided be "proportionality, reasonableness and actions that serve legitimate public interests".

Notwithstanding the need to balance multiple priorities, we suggest that the proposal creates additional uncertainty. While the Discussion Paper has identified that innovation, commercial processes and normal business functions are a matter of the public interest, it is unclear how far this concept would extend. As discussed above, the public interest is served by private commercial processes as these lead to the creation and refinement of products, services and technologies. The Insurance Council views that a key challenge for the proposals is to bridge the gap between theoretical privacy protections and practical business operations – particularly for entities that operate in data-heavy environments.

While the rest of the submission draws attention to some of these challenges, we view that the addition of an undefined "public interest" into the Objects of the Act is likely to further complicate rather than clarify this situation.

Therefore, the Insurance Council **recommends** that the "public interest" addition is not included in the Objects of the Act. In the alternative, we **recommend** that the OAIC develop guidance that clarifies how and when organisations can serve both the "public interest" and "privacy" when making operational decisions.

Proposal 2: Definition of Personal Information

2.1 Change the word 'about' in the definition of personal information to 'relates to'.
2.2 Include a non-exhaustive list of the types of information capable of being covered by the definition of personal information.
2.3 Define 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly. Include a list of factors to support this assessment.
2.4 Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.
2.5 Require personal information to be anonymous before it is no longer protected by the Act.
2.6 Re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments.

Insurance Council of Australia

With respect to expanding the definition of personal information to include "inferred or generated information", Insurance Council that this proposal would mean that personal information will not necessarily be attached to a person. To enable innovation and ensure that technology solutions can be sourced at speed (e.g., using Proof of Concepts, test cases) that pseudonymised, de-identified or anonymised data sets continue to be exempted from requirements under the Privacy Act.

Proposal 2.5, to require personal information to be anonymous before it is no longer protected by the Act, may present practical operational challenges due to the lack of alignment with existing industry and data standards. The Discussion Paper states that:

- *Information would be considered 'anonymous' if it were no longer possible to identify someone from the information, considering the definition of 'reasonably identifiable' and the factors outlined in Proposal 2.3*

Proposal 2.3 states:

- *An additional definition could be added to the Act outlining that an individual will be 'reasonably identifiable' if an APP entity or a third party could directly or indirectly identify anyone from that information.*

And:

- *Information would need to no longer be related to an identified or reasonably identifiable individual, considering the above definition, for the Act to no longer apply.*

The list of factors that could be taken into account in determining whether an individual is "reasonably identifiable" are presently undefined but could include:

- *…the context in which the information is to be held or released, the costs and amount of time required for identification, and available technology.*

The Insurance Council considers that this would define anonymous in a different way to how it is defined in other technical contexts, such as standards in information technology or cyber security. In particular, global industry benchmarks for information and privacy management such as ISO 27001 and ISO 27701 do not require this level of protection to mitigate privacy risks. The precise standard required under the proposals will be hard for entities to determine and the move to the term "anonymisation" is likely to raise expectations as to the level of protection. This also raises operational questions – the disjuncture between accepted technical standards and the legislated approach may create complexity and complicate implementation. As such, further consultation and sufficient implementation timeframes will be necessary.

Importantly, anonymity is contextual. Certain information may be anonymous within one set of circumstances but identifiable in another. For example, information could be considered "de-identified" while it is held by an APP (Australian Privacy Principle) entity. However, were that information to be released more generally, then the addition of more information could render it re-identifiable. The same example even applies internally within APP entities. One team may be working with a set of de-identified data within a sandbox environment. However, the addition of

Insurance Council of Australia

data possessed by another team in the same entity (eg. an IP address) could render the data re-identifiable.

Further, it can be functionally difficult for entities to determine if information has been definitively de-identified. Techniques may develop in future that could be used to re-identify individuals who were assumed to have been de-identified. We further note that including inferred or generated information could cause practical challenges with notification and consent proposals.

A final consideration relates to the question posed in the Discussion Paper (page 34) as to whether financial information should be highlighted as sensitive personal information. The Insurance Council again notes some practical difficulties with this. First, financial data is often required as a chain of evidence for fraud matters. If the proposals entrench anonymisation too heavily, then they risk the possibility of losing this evidence. Second, there would need to be much more detailed consideration of the type of financial information that would be included as sensitive personal information. For example, would it include premium amounts, BSB and account number, or claims information? If it includes claims information, then motor vehicle repairers and claims handlers would become responsible for sensitive personal information. This may require a high degree of change management.

Finally, the Insurance Council believes that these proposals need to be supported by a more clearly articulated problem statement. Specifically, it is unclear whether the proposals are aimed at internal ***first-party*** use of data or are intended to rectify issues with ***third-party*** use of data. Clearer articulation of the expected outcome would assist.

The Insurance Council **recommends** that, in lieu of the proposed changes, further options are provided in a more comprehensive OAIC guidance, including de-identification, pseudonymisation and anonymisation.

In the alternative, if the proposals relating to anonymity are legislated, the Insurance Council **recommends** the following:

- clear guidance be developed in consultation with technology experts to align with global privacy management practices;
- the definition of “personal information” be revised to made clear that, to the extent that technical, inferred and generated information is not “reasonably identifiable” when processed in the absence of other information, it is not considered to be personal information;
- the proposed list of factors that is generated to support assessment of whether information or an opinion is “reasonably identifiable” incorporate practical guidance on the assessment of technical information, inferred information and generated information, and that further industry consultation be held on the generation of the “list of factors”; and/or
- that any “data subject rights” as outlined in the Discussion Paper are legislated.

Finally, the Insurance Council **recommends** that further consultations be undertaken on the implementation timeframes and appropriate commencement dates.

Insurance Council of Australia

Proposals 3.3 and 3.4: Disclosure of personal information when an Emergency Declaration is in force

3.3 Amend Part VIA of the Act to allow Emergency Declarations to be more targeted by prescribing their application in relation to:

- entities, or classes of entity
- classes of personal information, and
- acts and practices, or types of acts and practices.

3.4 Amend the Act to permit organisations to disclose personal information to state and territory authorities when an Emergency Declaration is in force

The Insurance Council supports the proposal to introduce additional flexibility in targeted emergency declarations (ED). The Insurance Council views that additional flexibility will provide decision-makers with more confidence to make EDs in a wider variety of cases.

Part VIA was initially introduced in recognition that section 16A did not provide sufficient certainty for entities involved in disaster recovery. The discussion paper notes that Part VIA has been activated in three situations – the 2009 Victorian bushfire season, 2011 Queensland and NSW floods and 2019-20 bushfires across multiple states. However, Australia is facing an increasing number of CAT events – and many serious events are not covered by such EDs. During these events, there is often a need to rapidly share information held (variously) between emergency services agencies, recovery agencies and insurers. This information sharing helps to create a rich view of the threat profile.

In the absence of an ED, insurers and other stakeholders are reliant on section 16A, which states:

- *the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.*

The high bar imposed by 16A can present obstacles to effective information sharing. It is often the ***combination*** of data from several sources that enables a clear view of the threat profile within a CAT situation. In the absence of such data combinations, serious threats are often not apparent. For example, this may include where emergency or recovery workers are at risk from asbestos. However, while most issues that arise within a CAT situation could ultimately be framed as relating to "life, health or safety of any individual, or to public health or safety", there is not always an immediate causal proximity. The heightened bar of "serious" further complicates the issue. It could be that an issue, if left unchecked, would develop into a serious threat over time. In such circumstances, it is often unclear whether the 16A conditions are satisfied. This can have a deleterious impact on the ability of insurers and other stakeholders to respond to an emergency.

Efficient and timely triage and ongoing assessments following a disaster must be a priority to ensure services from government, community and Insurance sectors are effectively deployed for the benefit of community. For example:

- Sharing rapid assessment data gathered by emergency and response services could speed up the insurance triage process and provide quicker settlements to the community; and

Insurance Council of Australia

- Sharing insurance claims data could assist with the identification of under-insurance and non-insurance and the deployment of government and community sector services.

Several recent examples highlight where the inability to effectively share data has been to the overall detriment of local communities include the following:

- It was unable to be established in a timely manner whether a family was uninsured, resulting in elderly and disabled family members living in a severely damaged home;
- The insurance status and/or claim settlement status of an abandoned hotel could not be shared, resulting in the derelict building remaining the ongoing responsibility of the local government; and
- Inability to share data resulting in no capacity to target identification of candidate properties for resilience grants.

We therefore agree that additional flexibility is needed, for example by introducing intermediate options. The Insurance Council therefore **supports** Proposals 3.3 and 3.4. As suggested above, we view that these Proposals would provide decision-makers with more confidence in making EDs in a wider variety of situations. Nonetheless, this remains contingent on those powers being activated. Given the increasing frequency of CAT situations in Australia, the Insurance Council suggests that further clarity around section 16A is needed as a fallback option.

Finally, much of the relevant data originates in State Governments, which are exempt from the *Privacy Act*. We suggest that this element requires further consideration, and we note our earlier Insurance Council **recommendation** to the Royal Commission into Natural Disaster Arrangements that the Commonwealth and State Governments establish an effective data-sharing framework. This would involve the OAIC and other relevant industry stakeholders (including the ICA) working to identify and remove impediments in the *Privacy Act* to the development of an effective data-sharing framework.

Proposals 8 and 9: Notice of collection of personal information and Consent to the collection, use and disclosure of personal information

8.1 Introduce an express requirement in APP 5 that privacy notices must be clear, current and understandable.

8.2 APP 5 notices limited to the following matters under APP 5.2:

- the identity and contact details of the entity collecting the personal information
- the types of personal information collected
- the purpose(s) for which the entity is collecting and may use or disclose the personal information
- the types of third parties to whom the entity may disclose the personal information
- if the collection occurred via a third party, the entity from which the personal information was received and the circumstances of that collection
- the fact that the individual may complain or lodge a privacy request (access, correction, objection or erasure), and
- the location of the entity's privacy policy which sets out further information.

Insurance Council of Australia

8.3 Standardised privacy notices could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording and icons. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised notices.
8.4 Strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of collection, or if that is not practicable as soon as possible after collection, unless:

- the individual has already been made aware of the APP 5 matters; or
- notification would be impossible or would involve disproportionate effort

9.1 Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action. 9.2 Standardised consents could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, icons or consent taxonomies. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised consents.

The Insurance Council reiterates our earlier view (expressed in our response to the Issues Paper) about the implications of introducing a requirement for express notice to be given when collecting information. Insurers do not collect information for the purposes for large scale aggregation, but for the specific purpose of delivering insurance products and/or services to them. The new notice proposals and consent proposals could complicate the customer experience, increase the burden on business and introduce notice fatigue by increasing the requirements in situations where it is not useful. In circumstances where information collected is minimal, notices may not be necessary. Such examples could include:

- Where a customer makes an online social media query or post, a third-party witness for an insurance claim;
- Third party information gathered during a claims investigation; and
- Where multiple service providers are involved in a supply chain.

Issues also arise around collection, use and disclosure of information involving:

- Where third parties respond to claims made by them against an insured party, particularly in professional indemnity and other liability contexts; and
- Complex claims processes where information is collected, used and disclosed by a variety of parties, including insurers, claims adjusters, investigators and independent medical experts.

We reiterate our view that any move away from a principles-based approach towards standard forms requires careful consideration. The current regime allows insurers (and other APP entities) to appropriately tailor privacy notices, taking into account their own consumer research and other regulatory requirements. We draw the Department's attention to section 1012G of the *Corporations Act*, which recognises the need for flexibility in providing a customer with written notification requirements.

Insurance Council of Australia

Within Proposal 8, there is a tension between the stated goals of "clear, current and understandable" consent notices and other proposals, which are likely to increase "notice fatigue". More information does not necessarily translate to greater consumer understanding or awareness. Indeed, the likelihood is that it is likely to ***decrease*** consumer engagement – particularly for sectors such as insurance where there are already legislated requirements for consumer disclosure. While Proposal 8.2 attempts to limit the information required, in reality the listed information requirements could still require a potentially lengthy disclosure (for example, to cover off on purposes, third parties, and so on).

With respect to Proposal 8.3, the Insurance Council notes that insurers already operate under disclosure requirements imposed by the *Insurance Contracts Act*. Any standardised privacy notifications would need to consider existing requirements. We agree with the need for rigorous consumer comprehension testing – but also note that consumer comprehension testing will have to accommodate sector-specific requirements and will need to be undertaken in real-world scenarios.

Similarly, Proposal 8.4 seems to contemplate a much higher test than currently exists. It could significantly increase notice requirements that are not necessary or useful. A scenario where a new collection notice has to be provided prior to every customer interaction or when new information is "inferred" without customer interaction is not an optimal outcome. While there is an exception where an individual has already been made aware of APP 5 matters, in practice a long period of time between customer interactions usually requires re-provision of the notice. Insurers may only interact with customers once every twelve months (for renewals) and may collect different information from customers at different points. Further, the information that is collected at times of purchase/renewal is very different to that collected during claims. Collections may also be from non-customers where it may not be necessary or practical to provide a collection notice. Further clarity is needed to ensure that appropriate flexibility remains., noting that Proposal 8.4 currently does not appear to allow scope ***not*** to provide notice in appropriate circumstances.

Proposal 9 appears to be worded to require express consent in all circumstances that consent is required. This is a significant departure from the current ability to rely on inferred consent in appropriate circumstances. This raises a risk of consent fatigue if insurers were required to seek specific express consent every time and renew periodically (which would be additive to other statutory customer notice requirements).

The Insurance Council **recommends** that the AGD consider whether measures around notices of collection of personal information and consent proposals could be included in APP Codes for specific entity classes where it is identified that these additional obligations are necessary.

Proposal 10.1: The Fair and Reasonable Test

> 10.1 A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.

Proposal 10.1 seeks feedback on the introduction of a "fair and reasonable standard" that would cover all collection, use or disclosure of personal information under APP 3 and 6. This would be

Insurance Council of Australia

additional to the existing requirements under those APPs. The Insurance Council understands that the introduction of this test is to place more onus on APP entities to change their behaviour, thereby avoiding heavier reliance on consent.

As noted above, the Insurance Council views that a principles-based approach is appropriate for complex, economy-wide legislation of this nature. We suggest that additional guidance will be needed to support the introduction of broad-based principles such as those outlined in Proposal 10.1 In the absence of additional guidance, this proposal may add ambiguity and complexity. The introduction of a "fair and reasonable" test would provide scope for additional litigation as the term would need to be defined by courts. It is also unclear how the proposal would interact with "good faith" use in line with requests from regulators about use of data. For example, if a regulator approached insurers with a request for identification of customers experiencing vulnerability (or for another public policy purpose), it is not clear this would constitute fair and reasonable use of data. A range of complexities also arise around the involvement of reinsurers who require data under treaties with insurers to assess claims exposures.

Insurance Council An alternative approach is to streamline and strengthen existing requirements. By way of illustration, Chapter 2 of the European Union General Data Protection Regulations outlines all factors to be considered in decision-making.[3] A similar approach in this instance could assist simplification, which would both support understanding and confidence for both consumers and businesses.

The Insurance Council therefore **recommends** that any revision to the Act in relation to APP 3 and 6 to require 'fair and reasonable handling' streamlines these requirements to simplify the steps required to confirm the permissibility of handling, rather than adding an additional step or complexity. The Insurance Council further **recommends** that AGD consider whether the Objects section of the Act would be a more appropriate location. Finally, should the AGD proceed with the proposal in its current form, the Insurance Council **recommends** that a general "good faith" exception be introduced.

Proposal 10.3: Third party collections

> 10.3 Include an additional requirement in APP 3.6 to the effect that that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3. Commissioner-issued guidelines could provide examples of reasonable steps that could be taken, including making reasonable enquiries regarding the collecting entities' notice and consent procedures or seeking contractual warranties that the information was collected in accordance with APP 3.

Currently, APP entities are required to take reasonable steps to satisfy themselves that the original collection was in accordance with APP 3. Proposal 10.3 in the discussion paper appears

[3] European Union, *General Data Protection Regulation* (link)

Insurance Council of Australia

to respond to concerns raised by the OAIC about third-party collection of data where "it was apparent that it was originally collected by unfair or unlawful means", including through data breaches.[4] The Insurance Council is concerned that this broad-brush approach does not effectively engage with the multi-layer operations of many businesses, including insurers. For example, in an insurance claim, personal information could be collected by:

- The insurer, directly from a customer;
- An authorised representative or claims fulfillment supplier, who then provides the information to the insurer;
- A third-party who then lodges the claim (such as a broker, repairer or intermediary) or a third-party acting on behalf of the customer (such as a lawyer or financial counsellor); or
- Independent medical experts and lawyers involving in assessing claims for an insurer.

The Insurance Council views that each organisation should be able to satisfy itself that reasonable steps have been taken, which is the current approach. The proposal risks creating unrealistic and impractical obligations to investigate the method of data collection by a range of third parties. Proposal 10.3 would encompass third-party collections by insurers but is ultimately responding to a separate concern.

If the AGD proceeds with this proposal, more consideration is needed regarding the relationship between the relevant entity and the party that is collecting the information. The terminology used in the proposals – "reasonable steps" – remains unclear. For example, would a contractual relationship with a supplier satisfy this test? Would additional auditing or monitoring be required? What level of checking would be needed in individual cases? What would constitute reasonable steps in instances where information is received from government entities (for example, CTP or workers compensation)? Other sections of the discussion paper discuss a level of "impossible or disproportionate effort", which appears to be a high bar.

The Insurance Council **recommends** that the AGD does not proceed with this proposal. In the alternative, we **recommend** that more detailed guidance is required on the precise level of due diligence and that this detailed guidance should consider the matters outlined above.

Proposal 14: Right to object and portability

14.1 An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information. On receiving notice of an objection, an entity must take reasonable steps to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection.

Insurance Council The identified concern is that a customer is currently asked to make a single decision (at a single point in time) on a broadly worded request for consent. In turn, this consent request can be used for a variety of purposes that may not have been apparent to the customer. Indeed, the proposal notes that the Act is silent on whether consent may be withdrawn, although

[4] Attorney-General's Department, *Privacy Ac Review – Discussion Paper* (link) p92

Insurance Council of Australia

OAIC guidance states that it can. Proposal 10.1 therefore aims to provide more explicit and granular customer control over information. The Insurance Council is therefore unclear as to the practical difference between the existing and proposed approach.

If insurers are barred from using personal data in a particular way due to a customer objection, then this will impact the insurer's ability to perform other tasks that may be of benefit to the customer.

Therefore, the Insurance Council **recommends** that consideration be given to considering the impact of other proposals that shape what the request would look like. The Insurance Council particularly notes that, as with the right to erasure (below), consideration would need to be given as to the impact on specific sectors.

Proposal 15: Right to erasure of personal information

15.1 An individual may only request erasure of personal information where one of the following grounds applies, and subject to exceptions:

- the personal information must be destroyed or de-identified under APP 11.2
- the personal information is sensitive information
- an individual has successfully objected to personal information handling through the right to object (see Chapter 14)
- the personal information has been collected, used or disclosed unlawfully
- the entity is required by or under an Australian law, or a court/tribunal order, to destroy the information, and
- the personal information relates to a child and erasure is requested by a child, parent or authorised guardian.

15.2 Provide for exceptions to an individual's right to erasure of personal information. An APP entity could refuse a request to erase personal information to the extent that an exception applied to either all or some of the personal information held by an APP entity.

15.3 An APP entity must respond to an erasure request within a reasonable period. If an APP entity refuses to erase the personal information because an exception applies, the APP entity must give the individual a written notice that sets out the reasons for refusal and mechanisms available to complain about the refusal, unless unreasonable to do so.

The proposal for a consumer right to erasure would not extend to situations where the information is needed for the performance of a contract or in ongoing litigation. The Insurance Council agrees with these exceptions and suggests that any "right to erasure" would need to be carefully considered and worded so as not to impact legitimate business purposes that do not materially impact on privacy concerns.

We have identified the following examples:

- **Reinsurance.** In order to mitigate against their own portfolio risks, insurers will often seek reinsurance. For some product lines, the reinsurer may require insurers to provide information about high value claims;

- **Actuarial Models.** Personal information that has been de-identified and included in an actuarial model;
- **Prudential and Other Requirements.** Requirements imposed on insurers to hold data, including for audits, etc. Businesses should be able to reasonably service an erasure request in line with their current regulatory obligations; and
- **Risk Mitigation Activities.** Insurers may use information as part of risk management/ mitigation activities. A right to erasure could create obligations to cease use of this material, however de-identified, and attempting to identify where it has been used some time later may be very difficult.

For each of the above examples, there is no material impact on privacy concerns. However, they clearly illustrate potential business impacts that could arise from overly broad wordings.

Consumers should be given clear advance notice of the impacts of erasure. For example, it could limit the ability for the insurer (or other entity) to provide information to the customer in future. Alternatively, erasure of data could also limit the insurer's ability to perform other tasks that may otherwise be to the benefit to the consumer such as remediation. Clear advance warning would enable consumers to make informed decisions. This is also required to manage consumer expectations – if insurers are regularly managing deletion requests than consumers who have made such requests may need to lower their expectations around data portability and availability. These matters should be made clear to consumers.

Further, the Insurance Council notes some practical concerns. Some start-ups now offer a service in which they scan an individual's email inbox and send automated requests for deletion to companies that may have collected their personal information in the past. However, from the perspective of an APP entity, the incoming deletion request (that is, the automated deletion request sent by the start-up) typically has no customer information attached other than a name and email address. It is difficult for APP entities to even consider whether information could be deleted on that basis, as it raises serious questions around authentication and validation. This will pose additional challenges for insurers with a global presence. This illustrates how practical considerations around validation and authentication will need to be considered.

The Insurance Council **recommends** that the "possible further exemptions" (listed on page 122 of the Proposals Paper) could be extended – for example, where retention is required under an Australian law or legitimate contractual/prudential obligations, where erasure would pose a serious threat to the life, health or safety of any individual, where information has been de-identified, where it is impractical or unreasonable, or in cases where the policy is jointly held but the insurer has a reasonable basis for believing that one of the insured is subject to domestic violence. This would enable businesses to reasonably service an erasure request in line with their existing regulatory obligations and with minimal harm to individuals.

The Insurance Council further **recommends** that more detailed consideration is needed on operational questions such as ***who*** will have the right to apply for erasure of information. For example, will it extend to personal representatives of an individual? If so, this should include consideration of the potential risk of abuse if persons other than the individual request the deletion of data.

Insurance Council of Australia

Proposal 16: Direct marketing, targeted advertising and profiling

16.1 The right to object, discussed at Chapter 14, would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing. An individual could still request not to receive direct marketing communications from an organisation. If an organisation provides marketing materials to an individual, it must notify the individual of their right to object in relation to each marketing product provided. On receiving notice of an objection, an entity must stop collecting, using or disclosing the individual's personal information for the purpose of direct marketing and must inform the individual of the consequences of the objection.
16.2 The use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected.
16.3 APP entities would be required to include the following additional information in their privacy policy:

- whether the entity is likely to use personal information, alone or in combination with any other information, for the purpose of influencing an individual's behaviour or decisions and if so, the types of information that will be used, generated or inferred to influence the individual, and
- whether the entity uses third parties in the provision of online marketing materials and if so, the details of those parties and information regarding the appropriate method of opting-out of those materials.

16.4 Repeal APP 7 considering existing protections in the Act and other proposals for reform.

While the Insurance Council does not oppose the repeal of APP 7, we have concerns about the operation of associated Proposals 16.1 to 16.3.

Proposal 16.2 recommends that the purpose of influencing an individual's behaviour or decisions must be a primary purpose. Currently, many insurers view marketing as a secondary purpose, related to the primary purposes of providing and managing products and services. Marketing and targeting to influence a purchasing decision is likely a common purpose across all commercial businesses, and would be expected by consumers, but this does not mean it should be characterized as a primary purpose. The Insurance Council is concerned that this proposal will confuse consumers about the true purposes for which their information is being collected.

Insurers use "personalisation" to inform and educate prospective and existing customers about relevant matters, such as the risks of under-insurance or how to select appropriate insurance in areas with high natural hazard risks. How this is done is subject to existing consumer protections which have been implemented in a broad range of regulatory and other obligations that Insurers must comply with, such as the design and distribution obligations in the *Corporations Act 2001*. Further, there are potential flow-on public policy impacts (two of which are outlined above) should consumers be encouraged to opt-out of an effective communication channel.

Proposal 16.3 is also likely to create confusion for consumers and add significant complexity to the privacy policy. This proposal is not consistent with aim of keeping policies clear and concise.

Most organisations will engage a range of third parties in the provision of online marketing materials. It would be impractical to list all third parties involved in the privacy policy.

There is also concern about the interaction of Proposal 16 with other proposals, which could result in severely limiting the ability for organisations to conduct legitimate marketing activity with real commercial detriment. For example, if the definition of personal information is extended to include targeted advertising of an unidentified individual, this would bring into scope many common digital practices that pose no real privacy risk. Also, the proposed unqualified right to object under Proposal 14 is much broader in scope to the existing opt out right under APP7, extending the reach to not only use and disclosure but also ability to collect personal information.

The Insurance Council considers that express consent should not be required for direct marketing purposes and that the existing recognition of implied consent strikes the right balance, incorporating transparency and reasonableness without mandating specific action and risking consent fatigue. The APP Guidelines contain direction around when a consent is valid and factors to consider but allow flexibility in application as is appropriate for principles-based law. Mandating express consent would also be out of step with other laws regulating direct marketing that recognise inferred consent, such as the *Spam Act* and *Do Not Call Register Act*.

Proposal 20: Organisational accountability

20.1 Introduce further organisational accountability requirements into the Act, targeting measures to where there is the greatest privacy risk:

- Amend APP 6 to expressly require APP entities to determine, at or before using or disclosing personal information for a secondary purpose, each of the secondary purposes for which the information is to be used or disclosed and to record those purposes.

The Insurance Council understands that the OAIC may, in future, require organisations to demonstrate control accountability in certain circumstances, including organisation-wide Privacy by Design and Privacy by Default processes. Further, in circumstances where organisations undertake "high risk privacy practices", it is intended that either organisations will be required to demonstrate a higher level of privacy risk mitigation ***or*** that individuals would have stronger rights in relation to how organisations handle their Personal Information.

The Insurance Council **recommends** that, if either option is legislated, the OAIC provides comprehensive guidance to ensure that applicability of the organisational accountability requirements (for example, restricted practices for "large-scale processing" as outlined in the Discussion Paper).[5] This will be essential in assisting organisations to identify where the obligation may intersect with their operations and the requirements to comply.

With respect to the proposed requirements to record secondary purposes for personal information handling within organisations, the Insurance Council notes that there is not currently a distinct regulatory requirement within the APPs to keep a "record of processing" of primary purposes, let

[5] *Privacy Ac Review – Discussion Paper*, p12, 94-95

alone secondary purposes. This new requirement would require significant investment and hamper organisational ability to utilise personal information they hold in accordance with business and customer needs. It would require further changes to core business practices regarding capture, recording, monitoring and reviews to meet these requirements rather than serving customers.

The Insurance Council **recommends** that no requirement to record "secondary purposes" is legislated.

Proposal 24: Enforcement

24.1 Create tiers of civil penalty provisions to give the OAIC more options so they can better target regulatory responses including:

- A new mid-tier civil penalty provision for any interference with privacy, with a lesser maximum penalty than for a serious and repeated interference with privacy.
- A series of new low-level and clearly defined breaches of certain APPs with an attached infringement notice regime.

24.2 Clarify what is a 'serious' or 'repeated' interference with privacy.

24.3 The powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 (Regulatory Powers Act) would apply to investigations of civil penalty provisions in addition to the IC's current investigation powers.

24.4 Amend the Act to provide the IC the power to undertake public inquiries and reviews into specified matters.

24.5 Amend paragraph 52(1)(b)(ii) and 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined:

- a declaration that the respondent must perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/those individuals.

24.6 Give the Federal Court the power to make any order it sees fit after a section 13G civil penalty provision has been established.

24.7 Introduce an industry funding model similar to ASIC's incorporating two different levies:

- A cost recovery levy to help fund the OAIC's provision of guidance, advice and assessments, and
- A statutory levy to fund the OAIC's investigation and prosecution of entities which operate in a high privacy risk environment.

24.8 Amend the annual reporting requirements in the AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground.

24.9 Alternative regulatory models

- Option 1 - Encourage greater recognition and use of EDRs. APP entities that handle personal information could be required to participate in an EDR scheme. APP entities that are not part of a recognised EDR scheme could be required to pay a fee for service to the OAIC as the default complaint handling provider if a complaint is made against them.

- Option 2 - Create a Federal Privacy Ombudsman that would have responsibility for conciliating privacy complaints in conjunction with relevant EDR schemes.
- Option 3 - Establish a Deputy Information Commissioner – Enforcement within the OAIC.

The Discussion Paper[6] identifies insurance as one of the key sectors for privacy complaints. As an initial comment, the Insurance Council notes that this relies on data taken from the 2019-20 Annual Report, whereas the more recent data indicates that insurance is no longer one of the top sectors for complaints. The blanket description of the "insurance" sector does not allow for differentiation between different sub-sectors – such as general insurance, life insurance, health insurance and so on. Any consideration of "high privacy risk" should give appropriate weight to both volume of complaints received, volume of notifiable data breaches, appropriate definitions for each industry and weighting of complaints compared to the size of the industry and volume of customer interactions. As such, it will be important to ensure that these industries are defined clearly, that their inclusions are reasonable and that the reasons qualifying them for inclusion are appropriately considered and well-understood.

It is important to recognise that insurance is already a mature and tightly-regulated industry. Insurers are subject to APRA's CPS 234 (Information Security) which overlaps with other privacy regulatory obligations to a degree. General insurers are members of the Australian Financial Complaints Authority (AFCA), which provides an avenue for external dispute resolution and can hear cases involving privacy breaches.

Further, the volume of privacy complaints reflects not only the risk environment within a given industry but also the level of consumer awareness about legal rights and privacy breaches. Conversely, a low volume of complaints does not necessarily reflect a "low risk" industry – it may reflect that consumers in that industry are unaware of their rights or unaware of when their personal information has been violated. Additionally, the Insurance Council notes that the functions of the OAIC will remain economy wide. This should continue to be reflected in the imposition of the levy.[7]

We note that the insurance industry continues to face multiple funding pressures from Government. Among other things, insurers are subject to the ASIC industry funding levy, the financial institutions supervisory levy, levies to fund the Australian Financial Complaints Authority (AFCA).

Similarly, the proposed Compensation Scheme of Last Resort would require the insurance industry to fund remediation of unpaid compensation determinations that it did not contribute to. These levies have a cumulative impact that will contribute to continued upward pressure on premiums, in an environment where insurance affordability is a key concern for governments. Further information is needed on the precise level of the proposed levies before additional commentary can be provided.

[6] *Privacy Ac Review – Discussion Paper*, p184
[7] Noting exceptions for small business, etc.

Finally, there is a question around the provision of cost-recovery for advisory style services. It would be a perverse outcome if organisations are discouraged from seeking advice by cost-recovery fees. While acknowledging the cost to the OAIC for providing these services, the Insurance Council also notes that there is a strong public interest in education regarding privacy rights. We further note that the expansion of the data economy, as contemplated by the Government's *Australian Data Strategy* will require a broader strengthening of privacy and data education across the economy. This suggests that improved public funding may be an appropriate option in lieu of an industry levy.

However, if an industry levy is introduced, the Insurance Council **recommends** that it be commensurate with the time that the OAIC spends in dealing with individual industries.

With respect to enforcement (Proposal 24.9), the Insurance Council supports **Option 1** – to encourage greater use of external dispute resolution (EDR) schemes. As the Discussion Paper notes,[8] the *Privacy Act* currently recognises AFCA as the EDR provider for the financial sector. Retaining and bolstering the role of AFCA would be a sensible outcome. Reflecting the policy desire for a "one stop shop" for consumer financial disputes, AFCA was created to replace a myriad of EDR schemes. Separating one class of consumer disputes from another has the potential to unnecessarily complicate EDR and consumer consumers.

Proposal 26: Statutory tort

26.1 Option 1: Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123.
26.2 Option 2: Introduce a minimalist statutory tort that recognises the existence of the cause of action but leaves the scope and application of the tort to be developed by the courts.
26.3 Option 3: Do not introduce a statutory tort and allow the common law to develop as required. However, extend the application of the Act to individuals in a non-business capacity for collection, use or disclosure of personal information which would be highly offensive to an objective reasonable person.
26.4 Option 4: In light of the development of the equitable duty of confidence in Australia, states could consider legislating that damages for emotional distress are available in equitable breach of confidence.

The Insurance Council reiterates its earlier position of caution against a new statutory tort of privacy. While this should not be a determinative factor in and of itself, introducing additional scope for litigation will place upward pressure on insurance premiums or result in excluding the tort from insurance coverage. Should a statutory tort be introduced, it should be confined to intentional or reckless invasions of privacy. Further, any such tort should explicitly exclude actions that may be brought under the direct right of action. Finally, the Insurance Council stresses the importance of a nationally consistent approach. Some of the Options suggest the possibility of fragmentation across state lines. This would not be an optimal outcome. It would result in public

[8] *Privacy Ac Review – Discussion Paper*, p184

confusion about the rights that they had and potentially encourage forum shopping for litigants. The Insurance Council strongly views that, should a statutory tort of privacy be introduced, it should provide consistent protections on a national basis.

With respect to the specific options outlined in Proposal 26, the Insurance Council provides the following additional commentary:

- **Option 1:** The Insurance Council suggests that the tort model (or similar) currently under consideration by the South Australian Parliament could be examined as the basis for national adoption.[9] This model is based on a reasonable expectation of privacy with serious intentional breach.
- **Options 2 and 3:** The Insurance Council does not view these options as optimal. Putting the onus for developing a tort of privacy on court processes would limit the opportunity for strategic development of the tort and limit the ability for the tort to be shaped by public input. Further, while common law solutions may develop, they would necessarily be limited to the facts of individual cases.
- **Option 4:** As above, the Insurance Council does not prefer this option as it may lead to inconsistent legal protections across different state jurisdictions.

Finally, the Insurance Council **recommends** that, if the AGD proceeds with a statutory tort of privacy that further consultations occur around the level of statutory damages.

Finally, with respect to the direct right of action, the Insurance Council notes that this needs to be considered in conjunction with the statutory tort. The Insurance Council **recommends** that the direct right of action and statutory tort should be mutually exclusive.

Question: Employee Records

With respect to the Discussion Paper's questions regarding employee records, the Insurance Council notes two related concerns – first, the impact on governance requirements and, second, potential operational impacts of the proposed changes.

With respect to governance, the proposed changes would provide employees with a right of access to their data. This would include a right to receive, amend and delete records in some circumstances. The Insurance Council notes that, particularly for larger entities, employee records may be substantial, varied and held by several different functions across a corporate group. These can include payroll systems, offshore records (noting that many insurers are subsidiaries of global parent companies), human resources functions, and so on. Collating and actioning these requests can be resource-intensive and time-consuming. The proposed changes would add an additional regulatory requirement in instances where equivalent or substantially similar avenues already exist (such as "notice to produce" requests).

With respect to operational impacts, the *Fair Work Act* already provides a range of protections for employee records. Insurers already take steps to protect employee confidentiality and have

[9] *South Australia Civil Liability (Serious Invasions of Privacy) Bill 2021* (link)

Insurance Council of Australia

experience in dealing with personal or sensitive information – in the context of investigations, disciplinary processes, whistle-blower matters, and so on. These various processes attract differing but appropriate levels of confidentiality with respect to personal or sensitive information, depending on the nature of the matter.

As an example of the practical impact of the proposals, the Insurance Council notes that insurers could be prevented from properly undertaking disciplinary action for financial fraud (or other misconduct) because a participant has refused consent to collection or use of their information. While these cases may be non-standard, insurers with larger employee headcounts are likely to incur potentially significant resource commitments in responding to requests (including putting in place appropriate governance arrangements), alongside impacts to people management.

The current employee records exemption is appropriate and existing legislation already provides a sufficient level of governance of personal and sensitive information. If the proposed changes proceed, the ICA's preferred position is to retain the employee records exemption as is, or in the alternative, apply only elements of the proposed changes that would not give rise to the governance and operational impacts flagged above.

Further comments

The Insurance Council makes the following high-level comments about the Discussions Paper:

- Any recommendations for new obligations should aim to avoid duplication with *Corporations Act* hawking and SPAM Act obligations.
- Regarding overseas dataflows, the Insurance Council notes that Proposal 22.4 goes further than current. Further consideration is needed to determine any impacts, particularly for different business lines and outsourced activities to different providers in different countries. Further, since personal information may be generated or inferred (see above), the specific information that may be disclosed may not be known at the time that notification is originally given. Changing this to "types of personal information" may assist.

Next Steps

We trust that our observations are of assistance. If you have any questions or comments in relation to our submission please contact Aparna Reddy, the Insurance Council's General Manager, Policy – Regulatory Affairs, on 02 9253 5176 or areddy@insurancecouncil.com.au.

Yours sincerely

Andrew Hall
Executive Director and CEO