CPA Australia Ltd
ABN 64 008 392 452

Level 20, 28 Freshwater Place
Southbank VIC 3006
Australia

GPO Box 2820
Melbourne VIC 3001
Australia

Phone 1300 737 373
Outside Aust +613 9606 9677
Website cpaaustralia.com.au

18 January 2022

Attorney-General's Department
Robert Garran Offices
3-5 National Circuit
BARTON ACT 2600

By email: PrivacyActReview@ag.gov.au

Dear Sir / Madam,

Submission on the Privacy Act Review

CPA Australia represents the diverse interests of more than 168,000 members working in 100 countries and regions around the world. We make this submission on behalf of our members and in the broader public interest.

While we do not provide comment on each of the proposals, we provide responses to specific questions and proposals and make the following recommendations:

- Recommendation 1: We recommend that the definition of sensitive information includes information that is generated, inferred, or can otherwise act as a proxy for sensitive information.
- Recommendation 2: We recommend the retention of the small business exemption. To improve privacy protections, the government should instead support small business and their advisers through information and education campaigns.
- Recommendation 3: We recommend that the design of standardised layouts, wording and icons be informed by research and testing that assesses consumer needs across all levels of digital literacy and experience.
- Recommendation 4: We recommend strengthening the definition of consent by requiring consent to be based on affirmative actions and by limiting the validity of consent to a specific time period.

CPA Australia's detailed perspectives on specific questions and proposals are provided in the attachment to this letter.

If you have any questions about this submission, please do not hesitate to contact Dr. Jana Schmitz, Technical Advisor, Assurance and Emerging Technologies at CPA Australia on jana.schmitz@cpaaustralia.com.au.

Yours sincerely

Dr Gary Pflugrath FCPA
Executive General Manager, Policy and Advocacy

Encl.

Attachment

Complete list of proposals

Part 1: Scope and application of the Act

2. Definition of personal information

Response:

The Act currently does not address how information like location data and transaction data can be used as a proxy for sensitive information. However, as the Office of the Australian Information Commissioner (OAIC) guidelines point out, personal information may be sensitive if it clearly implies a category of sensitive information.

We note that sensitive information is defined as personal data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sexual orientation. We believe that location and transaction data can infer all of the above and should therefore fall under the definition of sensitive data. Exacerbated by the pandemic and its lockdown, transacting and browsing online and disclosing location data (e.g., through check-ins to venues) has become daily routine for Australians. Such practices generate a wealth of sensitive information.

Recommendation 1: We recommend the definition of sensitive information includes information that is generated, inferred, or can otherwise act as a proxy for sensitive information.

4. Removal of the small business exemption

Response:

We do not support the removal of the small business exemption. The past two years have been very difficult for many small businesses. They need the 'breathing space' to focus on recovery and rebuilding rather than implementing new regulatory requirements.

We do however see the need to improve privacy protections. Therefore, we encourage the government to consider taking an educative approach on this issue for small business rather than a regulatory approach. This could involve funding for improved information and training for small businesses and their advisers on data privacy. Such training could involve steps on how to protect consumer privacy and the value to the business of such protections.

Soon to be published research from CPA Australia will show that concerns over data privacy and security are major barriers to technology adoption by business. Given this, we believe that focusing on educating small businesses and their advisers on how to improve privacy is more likely to meet the desired policy outcome than extending the privacy regime to such businesses.

We are aware that retaining the small business exemption creates complexities among businesses and consumers. However, on balance, the value of keeping small business compliance burden low outweighs reducing such confusion.

We note the OAIC statement that 'Consumer Data Rights (CDR) data provided to trusted advisors outside the CDR system should still be subject to a baseline level of protection, being the protections in the Privacy Act'.[1] The latter is only achievable, however, when all trusted advisers are considered 'APP entities' for the purposes of the Privacy Act. In practice that is not the case due to the small business exemption.

Addressing this concern does not require the removal of the small business exemption. As with tax file numbers, there may be ways to amend the law to define 'trusted advisors' under the CDR regime as APP entities (noting that many trusted advisers such as tax agents would already be APP entities as they handle tax file numbers).

If the government proceeds with removing the small business exemption, we suggest:

- a long implementation period to give small business and their advisers sufficient time to familiarise themselves with the requirements of the Privacy Act

---

[1] Office of the Australian Information Commissioner, 'OAIC Submission to the CDR Rules Expansion Amendments Consultation' (29 October 2020) <https://www.oaic.gov.au/engage-with-us/submissions/oaic-submission-to-the-cdr-rules-expansion-amendments-consultation/>.

- that the OAIC supports small businesses in the "onboarding" process by providing required resources (educational and financial).
- That the government funds the implementation of dedicated support within the OAIC for small businesses to assist them in complying with the Privacy Act requirements.

Recommendation 2: We recommend the retention of the small business exemption. To improve privacy protections, the government should instead support small business and their advisers through information and education campaigns.

Part 2: Protections

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.

Response:

We support standardised privacy notices including standardised layout, wordings and icons to assist with consumer comprehension. The wording, layout and icons should be informed by extensive research and testing. In this regard, we emphasise the importance of and need to include statistically relevant numbers of different groups representing Australian consumers. It is crucial to include representatives with different levels of digital literacy and digital experience and to capture those with vulnerabilities due to physical and/or mental illness.

Recommendation 3: We recommend the design of standardised layouts, wording and icons be informed by research and testing that assesses consumer needs across all levels of digital literacy and experience.

9. Consent to the collection, use and disclosure of personal information

9.1 Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.

Response:

CPA Australia supports the proposed definition of consent in the Privacy Act in principle.

We emphasis that for consent to be valid, it should be based on affirmative action and not on pre-ticked boxes. What is required is an opt-in mechanism rather than preselected opt out settings. Further, to be valid, consent must be in clear and plain language and separate from other matters.

Moreover, we recommend that APP entities clearly state for how long consent is valid.

Recommendation 4: We recommend strengthening the definition of consent by requiring consent to be based on affirmative actions and limiting the validity of consent to a specific time period.

10. Additional protections for collection, use and disclosure of personal information

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.

Response:

We support the proposal that, when collected by third parties, entities must take reasonable steps to ensure that the data was originally collected from the individual. By identifying and verifying the source of the data, data reliability is significantly enhanced.

To assist APP entities meet this proposed additional requirement, the OAIC should release guidance (including examples) on what would be considered 'reasonable steps'.

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.

Response:

We support the proposed right to object or withdraw as it enables individuals to exercise control over the use or disclosure of their personal information. We further agree with the OAIC, that APP entities should also be required to notify an individual of their right to withdraw consent, where consent has been obtained.

As with the above, the OAIC can assist APP entities to comply with this change by publishing guidance on what they would consider to be 'reasonable steps' to stop collecting, using or disclosing the individual's personal information.

15. Right to erasure of personal information

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.

Response:

We agree that APP entities must respond to an erasure request within a reasonably short period.

The government should clarify what they intend by 'written notice'. Does it include notice delivered via digital means?

22. Overseas data flows

22.1 Amend the Act to introduce a mechanism to prescribe countries and certification schemes under APP 8.2(a).

Response:

CPA Australia supports measures to ensure that personal information collected in Australia that is disclosed overseas is subject to the protections in the Act. We support the recommendation previously made by the Australian Law Reform Commission (ALRC), that government develop and publish a list of laws and binding schemes in force outside Australia that provide privacy protections similar to the APPs. Such measures would provide Australian APP entities with greater certainty that the overseas recipient does not breach the APPs in relation to the disclosed information.

22.2 Standard Contractual Clauses for transferring personal information overseas be made available to APP entities to facilitate overseas disclosures of personal information.

Response:

We support the introduction of standard contractual clauses (SCCs) for transferring personal information overseas. We expect such SCCs, which contain safeguards outlining how an overseas recipient of personal information is expected to handle disclosed information, to lead to a significant reduction of regulatory burden on APP entities as they would no longer have to negotiate appropriate data handling clauses with overseas entities. Businesses that do not routinely disclose personal information overseas would benefit from such measures.

Part 3: Regulation and enforcement

24. Enforcement

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

Response:

We support enhancements to the OAIC's powers. We suggest that the OAIC have the authority to initiate its own public inquiries and publish the results of such work. The responsible minister should also have the authority to suggest that the OAIC conduct public inquiries into specified matters.

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.

Response:

CPA Australia does not support this recommendation. This will result in an additional financial burden, particularly on smaller businesses – many of whom find it difficult to pass on such costs to customers.

Another potential consequence of such a funding model is that it may lead to businesses closing, particularly smaller APP entities. The ASIC industry funding model is one of the reasons given for the recent reduction in the number of financial advisers. This in turn has limited consumer choice, leading to greater concentration of market power.

Importantly, the entire Australian economy and community benefits from an effective privacy regime. The funding of OAIC should therefore continue to come from consolidated revenue rather than just APP entities.

We note that the government has announced a review of the ASIC industry funding model. Therefore, we suggest it would be premature to consider that model until such a review is completed.

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.

Response:

Our preference is for Option 3.

Option 2 could complement Option 3. We suggest that dispute resolution should be carried out by the OAIC. Another option could be giving such dispute resolution power to the Australian Small Business and Family Enterprise Ombudsman (ASBFEO).

We do not agree with Option 1 - the proposed compulsory participation in EDR schemes. We note that APP entities that are not part of a recognised EDR scheme would have to pay a fee to the OAIC each time a complaint against them is lodged. Depending on the number of complaints, the imposed cost could have unnecessary negative impacts on business, especially where the same complaint is lodged by multiple parties or are vexatious.

27. Notifiable Data Breaches scheme

27.1 Amend subsections 26WK(3) and 26WR(4) to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates.

Response:

While we recognise that the proposed amendments will increase compliance burden on businesses, we consider the proposed amendments as reasonable as they enhance transparency and public accountability.