29 March 2023

Privacy Act Review

Attorney-General's Department

3-5 National Circuit

BARTON ACT 2600

***via email**: privacyactreview@ag.gov.au*

Dear Sir/Madam,

The proposed removal of the small business exemption from the *Privacy Act 1988*, should be supported by education and tools for small business to meet their compliance obligations

Thank you for the opportunity to provide feedback to inform the Australian Government's response to the Privacy Act Review Report (the Report).

The Report makes 116 proposals, with an estimated 95 of these having a direct or indirect effect on small businesses' privacy obligations. These proposals are both substantial and complex and with a limited review period, it is difficult to comprehensively evaluate the impacts of the proposals on small business.

The proposal to remove the small business exemption will have a significant regulatory effect on the obligations of small businesses on how they record, process, and protect customers personal information. The proposed reforms are significantly different from how many small businesses are currently required to protect consumer's personal information. We recognise that there are small businesses who already seek to fulfill the objectives of the Privacy Principles as part of a broader commitment to good governance, because of the technology the business uses, requirements arising from international trade or in acknowledgement of a self-appreciation of the sensitive personal data the business collects and holds.

We acknowledge that with the widespread use of technology and the large quantity of data that is now stored and collected by business and government there is an expectation from the community that personal information should be protected by those organisations who collect personal details. Small business is no exception to providing necessary and appropriate protections to customers personal information that they collect and store. However, it is important the regulatory framework requiring small business compliance is proportionate to the level of exposure to privacy risk and that small businesses are equipped with the tools and knowledge by the Australian Government to meet their compliance obligations.

We recommend that the Australian Government and the Attorney-General's Department proceed cautiously with the proposed amendments to the Act. It is necessary for the Attorney-General's Department to continue to consult with small businesses to ensure the changes appropriately consider the available resources of small businesses and their exposure to privacy risk. Accordingly, we recommend:

1. Small business compliance obligations with the Act should be proportionate to the level of exposure to privacy risk. The Australian Privacy Principles (APPs) should retain flexibility to

enable small businesses to fulfill their obligation to notify and inform customers of the collection of their personal information in proportion to their risk profile.

2. Prior to the removal of the small business exemption, the Australian Government must conduct an extensive education program and equip the Office of the Australian Information Commissioner (OAIC) with the necessary tools and resources to support small business in meeting their privacy obligations. This should include:

   - a simplified checklist or flow diagram of the 13 APPs explaining the clear steps required to meet their privacy obligations

4. The OAIC, the Australian Cyber Security Centre (ACSC) and the Department of Home Affairs Cyber and Infrastructure Security Outreach network should conduct a coordinated education and awareness campaign on the importance of cyber security as a tool to protect small businesses digital information.

5. Prior to the removal of the small business exemption, the Attorney-General's Department should conduct a new privacy impact assessment of the proposed amendments to the Act on small business. The assessment must model the cost for small businesses to:

   - understand their new obligations under the Act
   - train staff on their obligations to comply with the Act
   - design practices, procedures, and systems to enable compliance.

6. The Australian Government must provide clear guidance for small business on the responsibilities of controllers and processors of personal information. The introduction of the controller and processor concepts into the Act would require further consultation with small business to ensure there is a clear understanding of the responsibilities and the distinction between the roles. Small businesses should be consulted further to mitigate against the risk of small business deferring or being discouraged from adopting digital technology that improves productivity.

7. After the removal of the small business exemption, breaches of the Act that occur in the first two years by small business should be considered unintentional by the OAIC and should not be penalised. Instead, the OAIC should provide education and assistance to help small businesses understand why they incurred a notifiable breach.

8. The Commonwealth, state and territory privacy laws should be harmonised, and the Consumer Data Right (CDR) rules should be reviewed to ensure that there is a consistent approach for safeguarding personal information. A consistent approach is necessary for small businesses to understand their compliance responsibilities.

9. The Australian Government should conduct a review of the effects of the removal of the small business exemption after two years. The OAIC should record notifiable breaches for small business and the Australian Government should use this information to evaluate if adjustments to the Act are necessary, or where small business requires further support and education.

Further details on the recommendations follows below:

1. **Small Businesses compliance obligations with the Act should be proportionate to their level of exposure to privacy risk.**

Many small businesses collect some form of personal information such as names, address details, phone numbers, email addresses and payment details. The information collected, the method of collection and the system for storage varies across industries and is unique to the individual small business. With the removal of the small business exemption and the proposed amendments to the clarification of personal information, the Attorney-General's Department should ensure that the Australian Privacy Principles retain their flexibility to enable small business to tailor their personal information handling practices to their diverse needs and business models.

It is important for the Attorney-General's Department and the OAIC when they are considering the implementation of the proposed reforms in the Report that they evaluate the effects on small businesses, the diversity of small business, their available resources, and the personal information they collect, handle and store. Small businesses lack the administrative and financial resources of their larger counterparts, the information they collect may not be as comprehensive, and their exposure to privacy risk may not be as high. Small businesses compliance obligations should be proportionate to their level of exposure to privacy risk.

2. **Prior to the removal of the small business exemption, the Australian Government must consult with small businesses regarding the implementation of the privacy proposals and provide a toolkit with templates, information guides and education resources.**

Prior to the removal of the small business exemption the Attorney-General's Department and the OAIC need to consult with small business to understand the effects of the proposals in the Report and if these can be implemented by small business efficiently. Several proposals are complex and administratively difficult for small businesses who do not have the resources and available time to understand and develop the procedures, processes, and systems necessary to meet the proposed privacy obligations. These proposals include but are not limited to:

- Proposal 4.2–4.9: Personal information, de-identification and sensitive information
- Proposal 7: Employee records exemption
- Proposal 11: Consent and privacy default settings Security Retention and
- Proposal 13: Additional protections
- Proposal 15: Organisational Accountability
- Proposal 18: Rights of the Individual
- Proposal 20: Direct marketing, targeting, and trading
- Proposal 21: Security, retention, and destruction
- Proposal 22: Notifiable data breaches scheme

The OAIC should be adequately resourced to support small businesses through the provision of a small business toolkit that includes procedural templates, information guides and checklists. The small business toolkit will need to be available to small business prior to the removal of the small

business exemption enabling them to comply with their obligations under the Australian Privacy framework. The toolkit could include the following:

- a simplified checklist of the 13 Australian Privacy Principles explaining the clear steps required to meet their privacy obligations
- a flow chart or online tool where a small business owner enters what sort of information they collect, and the tool informs the owner of what Australian Privacy Principles (APP's) they must comply with
- standard form templates for privacy policies and privacy consent notices
- best practice guidelines on how to de-identify information
- communication material on the changes should be shared with industry associations, the ASBFEO and the state small business commissioners to distribute to their networks

3. The Australian Government should conduct a coordinated educational campaign on how the reforms affect small business and the importance of cyber security as a tool to protect small businesses digital information.

With an increasing government and business focus on cyber security and the protection of personal information, small business owners are increasingly becoming aware of the risk to their business systems and the information they hold. However, small businesses are not confident in their understanding of cyber security risks as found in the ACSC small business survey conducted in 2019.[1] Additionally, small businesses are not equipped with the resources or the expertise to understand the complexities of cyber security such as knowing what operating system they are using or the differences between the nine types of cyber security risks.

The proposed reforms in the Report will add to the already complex technical understanding required by small business to meet compliance obligations of the Act. The OAIC, the ACSC and the Department of Home Affairs should collaborate to deliver a joint strategy to increase the capability of small businesses to understand cyber security risk and how they can implement good cyber security practices to protect their systems and the digital information they store.

4. Prior to the removal of the small business exemption, the Attorney-General's Department must conduct a new impact analysis of the proposed amendments to the Act on small businesses.

Small business owners are often responsible for understanding compliance obligations amongst other administrative tasks such as workplace relations where their larger counterparts have the appropriate personnel to understand these complex issues. The proposed reforms in the Report will require small businesses to have technical knowledge and expertise, sufficient time to understand the effects on the business and what processes should be developed to meet their compliance obligations. The Attorney-General's Department must undertake further consultation with small businesses regarding the implementation of the proposed changes to ensure the minimum effective intervention.

[1] Australian Cyber Security Centre, *Cyber Security and Australian Small Businesses – Results from the Australian Cyber Security Centre Small Business Survey*, November 2020, accessed 24 March 2023.

Therefore, it is necessary for the Attorney-General's Department to conduct a comprehensive cost-benefit analysis of the proposed reforms to the Act for small businesses. The analysis must model the cost to small business to:

- understand their new obligations under the Act
- train staff on their obligations to comply with the Act
- design practices, procedures, and systems to enable compliance

5. The Attorney-General's Department should engage with small businesses across a wide variety of industries to determine the effect of introducing the concept of controllers and processors of personal information

The proposal to introduce the concept of controllers and processors of personal information into the Act may have the effect of discouraging small businesses from adopting digital technology that improves productivity if consultation is not undertaken with small businesses. Many small businesses rely on third party software to conduct their business and are of the understanding that the responsibility for privacy is with the software provider, due to the personal information that is captured by the software application. The proposed reforms, whilst intended to align Australia's privacy framework with international standards such as the General Data Protection Regulation, present a high risk of confusion for small business on the ownership of responsibilities for privacy controls.

Without consultation to understand how small business use third party software or provide software as a service to other businesses there is risk that innovation may be stifled. In our stakeholder consultations, concerns were raised that if education was not provided to small businesses, then there is a high risk they will become confused and may be deterred from adopting innovative software that will improve productivity. The Attorney-General's Department must consult further with small businesses to understand the effects of implementing this proposal on small businesses.

6. After the removal of the small business exemption, breaches of the Act that occur in the first two years by small business should be considered unintentional by the OAIC and should not be penalised.

In considering how best to assist small businesses to meet their requirements under the Act, it is important to strike a balance between enforcing regulations and providing support to small businesses to comply. The OAIC's Privacy Regulatory Action Policy currently employs an enforcement pyramid model that encourages compliance through education and support before penalising non-compliant businesses. This recognises that small businesses may breach privacy regulations unintentionally and may benefit from guidance on how to best meet their obligations under the Act. Assisting small businesses to meet their compliance requirements empowers small businesses to better protect the privacy of the Australian public.

7. Commonwealth, state and territory privacy laws should be harmonised, and the CDR rules should be reviewed to ensure that there is a consistent approach for safeguarding personal information

The proposed removal of the small business exemption will increase the already complex regulatory environment for privacy laws in Australia. Currently there are overlapping state and territory and Commonwealth laws that regulate the protection of personal information, such as:

- the CDR rules
- laws governing the collection and management of health records in NSW, VIC, and the ACT
- laws governing the use of surveillance devices in various states and territories.

Whilst we recognise that each regulatory framework addresses slightly different information management risks, complexity is increasing and making compliance for small business more challenging. The Attorney-General's Department should review and where possible harmonise the privacy laws, to reduce the complexity and confusion for small businesses who may have multiple compliance obligations.

8. **The Australian Government should conduct a review of the effects of the removal of the small business exemption after no more than two years.**

Reviewing changes to the Act after no more than two years provides the Australian Government with an opportunity to evaluate where and why small businesses are struggling to comply with the Act. In particular, the OAIC should record the notifiable breaches for small businesses and identify trends on how and why breaches are occurring. This will enable the Australian Government to understand what resources small businesses will need to meet their requirements under the Act. Ensuring small businesses can meet their compliance obligations under the Act is an important and necessary step to protect the privacy of Australian consumers.

Thank you for the opportunity to comment. If you would like to discuss this matter further, please contact Donna Boulton on 5114 6123 or at Donna.Boulton@asbfeo.gov.au.

Yours sincerely

The Hon Bruce Billson

Australian Small Business and Family Enterprise Ombudsman