

Our advocacy team is based in Canberra

Email: ceo@cosboa.org.au
www.cosboa.org.au

Attorney-General Department

Via email: privacyactreview@ag.gov.au

30 March 2023

Dear Sir/Madam,

Re: Privacy Act Review Report 2022

Thank you for the opportunity to submit feedback on the Privacy Act Review Report 2022. The Council of Small Business Organisations Australia (COSBOA) appreciates the consultation process and the commitment to strengthening privacy laws. However, we express concern over the increased penalties and potential impacts of more complex data regulatory requirements on small businesses.

Our vision is for small businesses to be appropriately engaged in a scaled approach to data security and privacy. We believe that burdensome regulations, requirements, and penalties could lead to disengagement, resulting in a less secure and protected environment.

On behalf of COSBOA, this submission seeks to address the potential impacts of the proposals contained in the Privacy Act Review Report and provide evidence-based recommendations for improvement.

1. Introduction

1.1 Background

This submission is a response to the Privacy Act Review Report, which comes after two years of extensive consultation and analysis of the Privacy Act 1988.

The digital economy has brought numerous benefits, but it has also led to increased privacy risks, such as identity fraud, reputational damage, and blackmail, due to the generation, use, disclosure, and storage of large amounts of personal information.

Trust in technology is vital for fostering economic development. The challenge lies in realising the benefits of data-driven technology while safeguarding individuals' privacy – something of global concern.

The Report's proposals aim to align Australia's privacy laws with international standards, protect Australians' privacy, enhance cross-border data flows, and yield economic benefits for businesses and the nation as a whole.

1.2 Goal

Our submission supports Australian small businesses by advocating for a targeted educative services approach, investment in privacy infrastructure, and a balanced approach to penalties and reporting requirements.

2. Executive Summary

In preparing this submission COSBOA consulted with a range of stakeholders, including Tech Council of Australia (TCA), Communications and Information Technology Training (CITT), Australian Small Business and Family Enterprise Ombudsman (ASBFEO), CPA Australia, Pharmacy Guild, the Australian Hairdressing Council (AHC), Institute of Certified Bookkeepers (ICB), and DSPANZ.

2.1 Key recommendations

COSBOA's key recommendations for the Privacy Act Review Report 2022 are:

1. **Educative Services:** Implement comprehensive education programs and increase awareness of regulators' roles including communications, webinars and training modules.
2. **Consumer Confidence:** Introduce a voluntary privacy certification scheme and a Small Business Privacy Code.
3. **Penalties:** Adopt a tiered model for maximum penalties and provide guidance and support from the OAIC, including a low-level infringement notice regime.
4. **Small Business Exemption:** Retain the exemption or provide ample implementation time and support if removed.
5. **Reporting Requirements:** Review federal and state laws and implement robust reporting frameworks, ensuring reasonable and simple/high-level detail in notices
6. **Compliance Guidance:** Offer government-endorsed best practice guidelines and formal governance programs, including adopting a 'legitimate interests' basis.
7. **Continued Consultation:** Engage with industry stakeholders for informed policy development and address specific concerns.

These recommendations aim to support small businesses while ensuring privacy protection and consumer confidence.

3. Issues and Recommendations

3.1 Issue 1: Promoting Awareness through Education

3.1.1 Background

The challenging business environment and recent data breaches highlight the need for improved privacy protections for both businesses and consumers.

3.1.2 COSBOA's Position

We propose a period of reprieve for small businesses to recover and build resilience, along with funding for better information and training on data privacy.

3.1.3 Evidence

Research from CPA Australia shows that data privacy and security concerns hinder technology adoption. Focusing on education is more likely to achieve desired policy outcomes.

3.1.4 Recommendation

Implement comprehensive education programs for small businesses and their advisers including communications, webinars and training modules, emphasising practical guidance, clear information, and risk mitigation strategies.

Increase awareness of the Commissioner's information gathering, sharing, and public statement powers, and clarify the roles of different regulators.

3.2 Issue 2: Enhancing Consumer Confidence

3.2.1 Background

Consumers increasingly consider data privacy in their choice of digital services, and small businesses often lack the resources to manage their privacy obligations effectively.

3.2.2 COSBOA's Position

We support introducing a voluntary domestic privacy certification scheme.

We support the development of a Small Business Privacy Code (SBPC), including a best practice guide and checklist for compliance.

3.2.3 Evidence

COSBOA's Cyber Wardens engagement & research shows that, while small business recognise the threats of cyber security, they lack the time, knowledge, and confidence to engage with them.

Through Cyber Wardens, COSBOA has engaged directly with small business, government, and industry to upskill the small business workforce.

3.2.4 Recommendation

In agreement with our association colleagues, we recommend a combined and collaborative scheme with Cyber Wardens complementing the SBPC.

This scheme would be overseen by the Office of the Australian Information Commissioner (OAIC), operate on a size proportionate 'cost recovery' basis, and offer a trust-mark logo to distinguish businesses with strong privacy practices.

3.3 Issue 3: Balancing Penalties and Support for Small Businesses

3.3.1 Background

The proposed increase in penalties and expanded powers for the Privacy Commissioner may disproportionately impact small businesses. The overall focus on consent in the new privacy act presents an increased burden for small businesses, as there is a higher need to obtain consent.

3.3.2 COSBOA's Position

We recommend a tiered model for maximum penalties, proportionate to the seriousness and frequency of breaches, and tailored to the entity type.

Furthermore, we advocate for the OAIC to provide support to small businesses in understanding and complying with privacy requirements including adopting a 'legitimate interests' basis, which is more business-friendly and flexible, enabling organisations to lawfully process data in a wider range of circumstances.

3.3.3 Evidence

The European Union's General Data Protection Regulation (GDPR) demonstrates a successful tiered model that ensures appropriate and proportionate penalties for various entity types, including small businesses.

3.3.4 Recommendations

Adopt a tiered model

We recommend the adoption of a tiered model for maximum penalties that is tailored to the entity type (companies, partnerships, microbusinesses, and sole traders), ensuring proportionate penalties are applied.

Address small business concerns

Address small businesses' concerns and uncertainties about the application and enforcement of privacy laws by having the OAIC play a more significant role in providing guidance on privacy compliance requirements and breach management.

Leverage trusted pathways

In addition to the recommended small business-specific education programs, leverage trusted pathways such as industry associations and advisors to disseminate information on compliance requirements and support for small businesses.

Offer clear guidance

Address potential conflicts arising from the Privacy Commissioner's increased powers by offering clear guidance on data sharing between agencies and the implications for small businesses, particularly start-ups.

3.4 Issue 4: The Small Business Exemption

3.4.1 Background

Removing the small business exemption under the Privacy Act 1988 will impose new costs and challenges on small businesses.

3.4.2 COSBOA's Position

COSBOA supports the retention of the small business exemption.

If the government proceeds with removing the small business exemption, we propose significant implementation period for education and training, scaled requirements, and dedicated support from the OAIC for small businesses.

3.4.3 Evidence

The review process' Discussion Paper highlights that small businesses are increasingly adopting digital services and may lack knowledge about data collection, storage, and obligations.

COSBOA's engagement with its members and small businesses has clearly demonstrated that many lack the expertise and resources to engage with this issue.

3.4.4 Recommendations:

Retain the small business exemption

To minimise the compliance burden on small businesses while recognising the potential for complexity between businesses and consumers, COSBOA's primary recommendation is that government retain the small business exemption.

If the exemption is removed, we recommend:

A significant implementation period

Ensure a significant implementation period for small businesses to familiarise themselves with the Privacy Act requirements.

Appropriately scaled requirements

Implement appropriately scaled requirements for small businesses that reflect their unique capabilities and resources.

Funding dedicated small business support

Establish and fund dedicated support within the OAIC to assist small businesses in complying with the Privacy Act requirements.

Encouraging investment in education & awareness programs

Encourage public and private sector investment in education programs to support small businesses in understanding and managing their data privacy obligations, particularly in the context of digital services.

3.5 Issue 5: Concerns Regarding Increased Reporting Requirements

3.5.1 Background

Small businesses face potential challenges from increased reporting requirements across various departments and states, and existing laws may be outdated.

Reduced timeframes result in less time for businesses to compile information required to provide a statement. This could be problematic for small businesses who generally have less capacity to dedicate to breach responses.

3.5.2 COSBOA's Position

The legislative reform process should review all data collection provisions and practices to ensure they remain reasonable and reflect the evolving privacy landscape. Additionally, the government should consider the level of detail required in notices and ensure that they are reasonable and simple/high-level.

3.5.3 Evidence

Recent incidents of data breaches and identity theft, such as those at Optus and Medibank, highlight the need for more robust legislation and defined reporting frameworks.

COSBOA's engagement with small businesses show that they are poorly positioned to tackle these reporting requirements, with many remaining confused about what they are expected to do.

3.5.4 Recommendations:

Review federal and state laws

As part of the legislative reform process to determine the reasonableness of current data collection provisions, review federal and state laws governing the collection, retention, and storage of personal and sensitive data.

Evaluate and update policy

Working with industry and stakeholders, re-evaluate and update policy and practices relating to data retention to ensure they remain relevant and effective.

Implement more robust legislated and defined reporting frameworks

To address the evolving threats to data privacy, provide clear guidance to small businesses, and improve consumer confidence, implement more robust legislation and defined reporting frameworks

3.6 Issue 6: Practical Advice for Small Business Compliance

3.6.1 Background

Compliance with data privacy legislation is an ongoing process., and small businesses must manage various aspects to prevent breaches and ensure adherence.

3.6.2 COSBOA's Position

To reduce small businesses' risk of contravening data privacy laws, legislative reform should be accompanied by government-endorsed best practice guidelines

3.6.3 Evidence

COSBOA's Cyber Wardens research and engagement demonstrate that small businesses lack sufficient knowledge regarding both their cybersecurity obligations and their access to data.

Fundamental knowledge such as what constitutes data, and whether a business holds any data, is lacking across all industries.

3.6.4 Recommendations

Provision of small business best practice guidelines

We recommend that legislative reforms should be accompanied by government-endorsed best practice guidelines to provide practical advice for small business compliance.

To ensure effective communication with small businesses, COSBOA strongly recommends that industry is consulted and engaged in developing these guidelines.

COSBOA's proposed framework:

- 1. Procedural Efficiency**
 - For ease of understanding, structure complex and wide-ranging data protection laws into manageable processes.
- 2. Risk Assessment**
 - Conduct comprehensive audits of privacy policy practices and procedures.
 - To ensure regulatory compliance and mitigate data breach threats, identify the biggest potential areas of risk.
- 3. Prioritise Risk Factors**
 - In a top-down approach determine which risk elements to address first.
 - Focus on breach-critical elements as the priority.
- 4. Understanding Data Collection**
 - Understand what data is collected, why, and for what purpose.
 - Be aware of data storage, sharing, and usage.
 - Comply with consumer requests for data access, editing, or deletion.
- 5. Establish a Formal Governance Program**
 - Demonstrate understanding and compliance measures to regulators.
 - Structure data capture, storage, sharing, and use procedures.
 - In line with the new legislative landscape, appoint a data protection officer to oversee day-to-day data collection and processing.

3.7 Issue 7: Need for continued consultation & engagement

Background

The current submissions process does not provide sufficient time for industry groups to effectively consult, engage with their members, and provide informed, evidence-based viewpoints back to government. This limited timeframe hinders the potential for a comprehensive and well-informed policy development process.

3.6.2 COSBOA's Position

Continued engagement and consultation with industry is crucial to ensure that policy development is informed by real-world insights and addresses the diverse needs of stakeholders. This collaborative approach fosters informed decision-making, addressing the dynamic needs of businesses and industries in Australia.

3.6.3 Evidence

In preparing this submission, COSBOA has consulted with a range of stakeholders, including Tech Council of Australia, Communications and Information Technology Training (CITT), ASBFEO, CPA Australia, Pharmacy Guild, and AHC. Time was regularly brought up as a limiting factor in addressing all relevant issues in the review.

3.6.4 Recommendations

Continue consultation & engagement with industry

To ensure policies remain relevant and effective we recommend continued consultation with industry stakeholders

We also note the following specific concerns, which due to time constraints, we were not in a position to address comprehensively:

- 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
- 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

4. Conclusion

In conclusion, while remaining concerned regarding the potential impact of increased penalties and complex regulatory requirements on small businesses, we do appreciate the Government's commitment to strengthening privacy laws.

Rather than focusing on fear-inducing penalties and onerous reporting regimes, COSBOA recommends, through education and risk mitigation, a supportive approach that empowers small businesses.

We support the introduction of a Small Business Privacy Code complemented by effective engagement with small business, as demonstrated by the Cyber Wardens pilot program.

Lastly, to ensure well-informed and effective policy development, COSBOA strongly advocates for ongoing consultation with small business stakeholders.

On behalf of our members, we sincerely thank you for the opportunity to participate in this consultation process.

Yours sincerely,



Matthew Addison
Chair of the Board
Council of Small Business Organisations Australia (COSBOA)

Secretariat: PO Box 463 Canberra ACT 2601 (+61) 493 364 720 Our advocacy team is based in Canberra
Email: ceo@cosboa.org.au/www.cosboa.org.au