Ai GROUP SUBMISSION

Australian Government
Attorney-General's Department

Response to the Privacy Act Review Report

March 2023

The Australian Industry Group (Ai Group®) is a peak national employer organisation representing traditional, innovative and emerging industry sectors. We have been acting on behalf of businesses across Australia for 150 years.

Ai Group and partner organisations represent the interests of more than 60,000 businesses employing more than one million staff. Our membership includes businesses of all sizes, from large international companies operating in Australia and iconic Australian brands to family-run SMEs. Our members operate across a wide cross-section of the Australian economy and are linked to the broader economy through national and international supply chains.

Ai Group supports the need to provide the public with confidence that their privacy and their data is being handled safely and responsibly. We advocate for the principle of Data Stewardship, which reflects the obligations and responsibilities of business of all sizes and industries in managing data collected in the usual course of business or as part of the business model. It reflects both the governance requirements and responsible utilisation of data and covers technological and behavioural strategies. It also addresses the safe disposal of data at the end of its usefulness.

Consideration should be given to the impact of multiple forms of regulation in this area such as Consumer Data Right and industry specific regulations. Over-regulation has the potential to chill innovation and add costs to business.

There are two significant changes presented in the report that business must grapple with:

- the inclusion of SMEs and
- the closer alignment with GDPR rules.

We maintain our objection to removal of the exclusion of SMEs. We acknowledge that there is support being offered to assist SMEs to comply with new regulations, however, it needs to be recognised that compliance to these rules is an ongoing adaptive process as technology and business practices change. Support cannot be regarded a 'set and forget' proposition, rather Government and industry must work in partnership for the long term to support privacy considerations without stifling innovation.

Ai Group has long advocated for international regulatory cohesion in digital and privacy rules. We welcome the attempt to align with the rules of our trading partners, however, there is a risk that we make limited facsimiles of external rules, with far reaching consequences in the Australian context, without achieving the benefit of automatic reciprocal coverage. The justified and welcome exceptions for employee data may risk the desired outcome.

Similarly, there should be caution against shifting emphasis of protecting consumers under the current regime, to data protection under the EU GDPR. The EU GDPR is a complex scheme with qualifications and exceptions to ensure practical implementation. Adoption of definitions and other individual features of the EU GDPR risks over-inclusiveness and unworkability.

Government should be aware of various issues associated with adopting an EU GDPR approach. International experience suggests that the EU GDPR has been highly prescriptive, with certain provisions introducing significant burdens on regulated businesses without necessarily providing demonstrable benefit to individuals. Retaining the flexibility of the APPs would mitigate the risk of a similar outcome in Australia.

Of particular concern is the introduction of a requirement of a **Data Protection Officer and a Data Impact Statement** and the risk of increasing the regulatory burden on Australian businesses, especially public facing businesses. As the OAIC prepares its guidance, we encourage lengthy consultation with a wide range of organisations to avoid regulatory overreach.

- Notice of collection of personal information:
    - Government should be cognisant of the risk of cumulative increase of notifications and information overload for consumers associated with notice of collection requirements.
    - Government should properly assess whether there are material consumer benefits from expanding the range of requirements for giving of notice of collection requirements, and as to the content of these notices.
- Consent to the collection, use and disclosure of personal information:
    - Government should be cautious to not add a costly regulatory burden to businesses by requiring the retrospective operation of consent requirements in relation to already obtained data.
    - Similar to the issue of notice of collection requirements, Government should be cognisant of the risk of creating information overload or consent fatigue for consumers with consent requirements.
    - There are practical implementation issues for businesses if the statute expands the range of requirements for obtaining of consent, or the form of requests for consent.
    - Opt-in consent should only be required where it is a real benefit to individuals and does not materially impact on the ability of businesses to provide and develop innovative services to the benefit of consumers and the broader Australian economy.
    - Government needs to properly understand the EU GDPR approach to consent. This includes the many exceptions and limitations to those consent requirements, including the legitimate interest exceptions.
    - Proposal 13.4 can be problematic for logistics service providers. They receive personal information about an individual from a third party (e.g. receive consignees' personal information from shippers). The proposal may have unintended consequences and/or burden for logistics service providers who have hundreds of thousands of consignments per week where the customer/shipper provides the personal information of the consignee/receiver to facilitate delivery. A requirement that the third party would need to verify consent could create a diffusion of responsibility and practical implications to the transfer of personal data.
- Right to erasure or be forgotten:
    - Consideration should be given to how erasure rights would impact insights that businesses develop through their own methods (e.g. inferences).
    - Proper consideration of public interest exemptions should be given to the right to erasure. This should ensure proper consumer safeguards are considered and not inadvertently impacted, such as ensuring privacy and security, preventing fraudulent activity and resolving complaints or litigation.
    - Introducing this right could create a conflict with providing incentives to entities to ensure effective anonymisation of personal information to better protect against privacy risks.
    - Introducing this right could also conflict with mandatory regulatory requirements for retention of personal data.
    - Unlike under the EU GDPR, the proposed right is not qualified through judicial oversight and

ability to make public interest considerations. This should be taken into account and amended.

- Direct marketing, targeted advertising and profiling

We appreciate the intention behind the proposal is aimed at assisting individuals in enhancing their awareness and understanding about the use of information for direct marketing. However, the proposal does not contemplate that such information is collected for other various legitimate reasons that would also be in the individual's interest. For instance, consumers could reasonably expect information to be collected to enable better customer service, improve products or service customisation, communication of non-marketing information such as invoices, and to protect against fraud. In this regard, loyalty schemes should benefit from being considered for exemption as an example. Such applications are not always known at the time of collection, which could evolve over time to meet consumer expectations. Careful consideration should be given to any opt out settings so that consumers and businesses can continue to benefit.

- Proposed removal of the small business exemption

Ai Group opposes the proposed removal of the small business exemption as identified in the Review Report at recommendation 6.1. The removal of the current exemption would impose a significant cost and compliance burden on small business that in many instances would be disproportionate to the incidence and scale in which personal information is collected.

The Review Report proposes that consultation with an impact analysis should occur before the current statutory exemption is removed. It is apparent that any impact analysis would only be accounted for in designing support measures as a result of the exemption's removal rather than in the design of an alternative or more narrow exemption. While consultation is welcome, this provides little comfort to small business operators, who would be greatly concerned about the magnitude of the compliance cost and viability of their operations.

Ai Group contends that the removal of the exemption would present very significant challenges for small business and their capacity to comply with the APPs. Small businesses cannot simply adopt the technological and digital infrastructure to comply as larger organisations. Similarly, the need to upskill and/or hire new staff to assist in the implementation of the APPs would be an essential step that many small businesses would not be in a financial position to take.

The removal of the current exemption would also be a strong barrier to small business creation and will no doubt create constraints on the ability of small business to grow and employ.

If, despite Ai Group's objection, the proposal proceeds, it is essential that consideration be given to an alternative level of privacy regulation that may go to modifying the exemption rather than its complete removal.

The Review Report's proposal at 6.2 states:

In the short-term:

- *prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption, and*

- *remove the exemption from the Act for small businesses that obtain consent to trade in personal information.*

While Ai Group consider these measures to be far more targeted and less disruptive to small

business across the board, the introduction of any new obligation on small business should be preceded by adequate consultation and with extensive transitional arrangements.

- Employee records exemptions

The Review Report proposes an increase in privacy protections for employees but acknowledges that "further consideration is required as to how the privacy and workplace relations laws should interact."

Specifically, the Review Report makes recommendation 7.1 in relation to the employee records exemption.

Enhanced privacy protections should be extended to private sector employees, with the aim of:

a) providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for

b) ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information

c) ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and

d) notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm.

Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact. The possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored.

Ai Group supports the retention of the current employee records exemption in the Privacy Act 1988 (Cth) (Privacy Act) and strongly opposes its removal.

Further, Ai Group does not support narrowing the employee records exemption (or the effect of the exemption) such that it would create additional obligations on employers that not only carry an added regulatory burden but constrain employers from acting in compliance with other workplace laws.

Ai Group refers to its earlier submissions regarding the importance of retaining the employee records exemption and its essential role in enabling employers to manage matters arising from the employment relationship and obligations under a variety of workplace laws.

If anything, under current Australian Government labour standards and gender equity policy, the need for employers to collect employee personal information relating to the workplace is growing. This reflects the intended outcomes of Government policy in often requiring higher levels of employer intervention and control into various workplace matters, rather than any commercial motivation of the employer.

For instance, recent legislative developments in the areas of workplace sexual harassment, workplace gender diversity reporting and foreshadowed reform concerning employer obligations relating to the underpayment of wages, same job same pay, labour hire licensing and modern slavery

due diligence all elevate the need for employers to be collecting employee information to help satisfy new and specific legal obligations.

It is essential that privacy reforms relating to employee information travel cohesively with current Government workplace reform -particularly given its magnitude.

Accordingly, it would be inappropriate and would add to the fragmenting of privacy obligations (as they relate to employers and employees) if any further reform around employee privacy protection was solely dealt within the Privacy Act. As referred in our earlier submissions, the Fair Work Act 2009 (Cth) regulates employer obligations in relation to employee and employment records, in addition to various state and territory workplace surveillance legislation.

If the Government is minded to engage in further consultation about modifying, or modifying the effect of the current employee record exemption, it is essential that it squarely focus on the impact of any proposed modification as it relates to the employment relationship, and employer (and employee) obligations under workplace laws.

The specific formulation of considerations in recommendation 7.1 would create a raft of problems for employers in managing matters arising in the employment relationship and workplace law obligations. What may be seen as a modest and targeted modification to the employee exemption may still have profound adverse and unintended consequences on a range of matters, such as employee and community safety.

For instance, we envisage that additional employer obligations arising from legislating matters in 7.1(a), (b), (c) and (d) would have the potential to significantly impede the ability to conduct workplace investigations (including work, health and safety) or other disciplinary matters employers may be required to act upon.

The role of privacy codes of practice may be a more appropriate and targeted alternative to new legislative obligations on employers. Ai Group would not support codes of practice if they were intended to add a further regulatory layer to any new legislative obligations on employers in respect of employee records and employee information. This would be of limited utility to employers and employees and would only add to the complexity of privacy regulation generally.

Ai Group would not be opposed to a tripartite consultation process given that the issues for consideration need to be properly understood as they apply to employers, employees and workplace laws.

It is essential that the workplace relations legislative framework remain the appropriate framework for any further assessment by the Government relating to privacy protections for employee records.

Louise McGrath

Head of Industry Development and Policy

Australian Industry Group.