Clubs Australia Submission
Government Response to the Privacy Act Review Report

Clubs Australia welcomes the opportunity to provide feedback on the Government response to the Privacy Act Review Report.

Clubs Australia represents 6,400 not-for-profit licensed clubs that provide their communities a range of hospitality, entertainment, social and recreational activities.

Clubs Australia supports a robust privacy framework that protects the privacy of individuals while also ensuring that regulatory requirements on business are proportionate and well-understood.

Summary of Recommendations

1. **Clubs Australia does not support removing the small business exemption. However, if the exemption is narrowed, small businesses should remain exempt from costly and regulatory requirements like having a privacy policy and issuing collection notices.**

2. **Clubs Australia supports retaining the employee records exemption and clarifying that collection of employee information is covered by the exemption.**

3. **Regarding facial recognition technology, Clubs Australia recommends:**

    a. **state and territory governments retain the power to authorise or require businesses to use the technology;**
    b. **privacy impact assessments for facial recognition technology be capable of being conducted on behalf of an industry, where the circumstances and risk profiles are similar.**

4. **Clubs Australia supports exemptions to right for individuals to seek erasure of their personal information, to ensure clubs can continue to meet their business and harm minimisation requirements.**

5. **Clubs Australia believes that any industry funding model should exclude businesses that do not commercialise or profit from personal information.**

Small Business Exemption

Small clubs tend to be run by volunteer directors, with many only open one or two days per week such as during weekend sports. Small clubs are also generally more reliant on membership subscriptions as a form of revenue because they conduct limited commercial activities. Small clubs are therefore sensitive to increases in the cost of doing business, as they are practically unable to scale up their services.

Removing the small business exemption threshold of $3 million annual turnover will result in approximately 5,000 small clubs incurring regulatory and other compliance costs, disproportionate to their size and risk profile.

For instance, small clubs would endure legal and professional costs developing and regularly reassessing an APP privacy policy, preparing privacy collection notices, as well as undertaking initial and routine privacy audits.

The need for smaller clubs to seek costly legal assistance would be exacerbated by the principles-based nature of the Privacy Act, which requires legal expertise to apply the legislation to the individual circumstances of the club.

The cost estimates in the Review Report of a $229.87 start-up cost and $391.79 ongoing cost are significantly less than the legal and consultancy costs necessary to prepare a privacy policy and privacy collection notices alone.

For instance, Clubs Australia estimates that consulting a law firm to prepare a privacy policy would cost at least $5,000 and reviewing or updating an existing policy costs $3,000-$4,000. These costs involve a review of the business's privacy practices and personal information flows and a risk assessment specific.

Any attempt to reduce these costs by creating a template policy will defeat the policy rationale of enhancing privacy practices, because template policies will disregard the specific circumstances of the business.

Clubs would also incur regulatory costs arising from training staff, handling complaints, as well as responding to requests for access to, or correction of, personal information.

As the threshold of $3m in annual turnover is not indexed, small businesses are already increasingly being brought into the APPs regime over time, particularly given high inflation levels. Three million dollars today is equivalent to $1.68m in 2000 when the Privacy Act was extended to the private sector.[1]

[1] RBA inflation calculator

If the Government decides to remove the small business exemption, Clubs Australia recommends that small businesses only be required to observe "negative" APPs, that prohibit, or set rules for, various acts. For instance, these include wrongly collecting, using or disclosing personal information, and adopting government related identifiers.

Clubs Australia recommends against small businesses being subject to "positive" requirements such as having an APP privacy policy, issuing privacy collection notices and responding to access and correction requests.

Clubs Australia does not support removing the small business exemption. However, if the exemption is narrowed, small businesses should remain exempt from costly and regulatory requirements like having a privacy policy and issuing collection notices.

Employee Records Exemption

Clubs Australia supports retaining the employee records exemption and clarifying that collection of employee information is within the scope of the exemption.

Amending the Privacy Act to narrow or remove the exemption will unnecessarily interfere with the employer-employee relationship. As detailed below, existing laws already govern an employer's handling of employee information, and the Privacy Act is unsuitable for governing these matters.

Existing laws

In assessing the merits of removing or limiting the employee records exemption – as well as extending the exemption to collection – it is necessary to evaluate the existing laws which may govern an employer's handling of employee information.

Clubs Australia's submission to the Discussion Paper sets out these existing protections, as summarised below:

- **Privacy Act**: The limited application of the employee records exemption means that employers who misuse an employee's information cannot necessarily rely on the exemption.[2]
- **Work, Health and Safety law**: The model Work, Health and Safety Act already imposes a positive duty on employers to minimise any risks to employees' health and safety.[3] Employers who fail to protect their employees' information, or who misuse their information through disclosures to third parties, may be in breach of this statutory duty.

[2] QF & Others and Spotless Group Limited (Privacy) [2019] AICmr 20; B v Cleaning Company [2009] PrivCmrA 2.
[3] Section 19.

- **Fair Work Act**: Employers are prohibited from keeping false or misleading records of employees,[4] must make an employee record available to an employee for inspection and copying on request,[5] and are required to correct employee records that contain an error.[6]
- **Common law**: Employees have an implied duty to follow a reasonable and lawful direction. Any request by an employer to collect personal information from an employee can be assessed against this duty.

The Privacy Act is unsuited to govern employer handling of employee information

The table below sets out just some of the challenges and considerations stemming from extending the APPs to an employer's handling of employee information.

APP obligation	Challenges
APP 3: collection of solicited personal information	• Subclause 3.2 requires the collection of personal information to be "reasonably necessary …". This requirement effectively duplicates a similar standard arising from common law in the context of workplace relations; that the collection must be lawful and reasonable. • Subclause 3.3(a) requires consent for the collection of sensitive information. It is unclear how an employer is to deal with a scenario where an employee does not consent, despite the direction from an employer being lawful and reasonable. • Subclause 3.6 requires an organisation to collect personal information about an individual only from that individual, unless it is unreasonable or impracticable to do so. This exception would commonly be enlivened where an employer conducts a performance review (e.g. 360-degree feedback) about an employee, or conducts a workplace investigation. Where there are multiple hierarchical management tiers in an organisation, senior managers may commonly "check up" on an employee by asking the employee's manager for an update. The expansive definition of personal information means that any opinion or information about the employee or their performance would need to satisfy the exception in subclause 3.6(b). Accordingly, employees would constantly be assessing this exception every time they email or document information about a work colleague, subordinate or manager.

[4] *Fair Work Act 2009* (Cth) s 535(4).
[5] *Fair Work Regulations 2009* (Cth) reg 3.42.
[6] Ibid reg 3.44.

APP obligation	Challenges
APP 5: notification of the collection of personal information	• Removing the employee records exemption will require employers to give employees a privacy collection notice every time they seek personal information. Given the regularity with which many employees submit personal information to their employer in the course of work, requiring a privacy collection notice is impractical and onerous.
APP 6: use or disclosure of personal information	• Employers may disclose an employee's personal information to multiple other parties such as organisations providing workforce management services (e.g. payroll, rostering etc.) or other HR services like training, coaching and performance management. Subclauses 6.1 and 6.2, effectively require an employer to obtain an employee's consent before every disclosure unless the employee "reasonably expects" the employer to disclose this information, and the disclosure is sufficiently "related" to the primary purpose.
APP 12: access to personal information	• Empowering an employee to request access to their personal information is clearly inappropriate in some scenarios, such as where the information is a performance assessment, reference from a referee, or if the information was provided during a workplace investigation.
APP 13: correction of personal information	• Similar to the challenges that would be posed under APP 12, it would also be inappropriate if an employee is empowered to seek to correct information such as a performance assessment or evidence from a workplace investigation.

Accounting for these challenges would create a predicament. Either the APPs would shoehorn the unique features of workplace relations practice into the principal rules and exceptions, by modifying existing provisions. This approach would potentially dilute or modify the application of the APPs to the handling of personal information outside employment settings.

Alternatively, the APPs could create new rules and exceptions where workplace relations practices necessitate changes. This approach would expand the list of rules in the APPs and create further confusion and complexity.

Notwithstanding these practical challenges, amending the laws governing the handling of employee records in the Privacy Act fundamentally misunderstands the employment relationship.

There are several distinguishing factors about the employment relationship:

- The employment relationship is defined by an employment contract featuring protections and express and implied rights and duties. Conversely, other relationships governed by the Privacy Act – such as those between a business and consumer, client and user – do not feature similar protections and rights recognised and enforceable by law. The Privacy Act fills an important gap with respect to these relationships, however this rationale is absent for the employment relationship.
- The employment relationship features mutual express and implied duties and obligations, unlike the relationships covered by the Privacy Act. As noted earlier, imposing further obligations on an employer – such as seeking consent to collect sensitive information – may interfere particularly with duties already owed by an employee to their employer.
- An employer already owes employees special duties such as good faith and fidelity/mutual trust and confidence. As the objects of the Privacy Act are focused only on the obligations in the legislation, breaches of the APPs will not recognise the special duty by employers.
- The remedies available to employees are more nuanced, reflecting the unique characteristics of the employment relationship. For instance, if an employee incurs some loss or unfavourable treatment because they refused an employer's request to send personal information, or because the employer holds incorrect information, the employee is likely to be interested in a remedy unavailable in and unconnected to the Privacy Act.

If, despite our submissions, any changes are to be made to private sector employees' privacy protections, any such amendments should be implemented through workplace relations laws.

Clubs Australia supports retaining the employee records exemption and clarifying that collection of employee information is covered by the exemption.

Facial Recognition Technology

Approximately 30% of Australia's clubs operate gaming machines and strong harm minimisation measures are pivotal to the industry's social licence. A robust self exclusion system is a key pillar of the harm minimisation mix. Under this scheme, those experiencing gambling harm can exclude themselves from gambling venues. Facial recognition technology (FRT) presents important opportunities for clubs to identify excluded patrons, prevent them from gambling and get them support.

To facilitate the adoption of this technology, Clubs Australia believes that the Privacy Act must include stronger safeguards and protections to ensure FRT meets community expectations and does not get misused.

For the purposes of our comments, we recognise that any law governing the use of facial recognition will include a threshold question on whether the business can use FRT, in addition to the settings and controls underpinning the use of the technology.

Threshold question

While Clubs Australia does not comment on the specific standards governing the threshold question, we believe that:

- clubs should be able to use FRT to identify excluded gamblers; and
- state and territory governments should retain the power to authorise or require businesses to collect sensitive information.

Regarding the powers of state and territory governments, clubs in South Australia that operate 30 or more gaming machines must have approved FRT installed in their gaming rooms under the *Gaming Machines Act 1992* (SA). This has been introduced to ensure that a patron who has self-excluded cannot enter a venue and gamble.

There are strict installation and operating requirements in relation to the use of FRT in South Australia venues, with clear guidance provided by the Government.

Clubs Australia recommends that states and territories should retain the power to permit facial recognition for use.

Settings and controls

Clubs Australia supports in principle a model-law approach to facial recognition. We consider the UTS Model Law includes a valuable set of risk-based legal requirements which provides an important foundation in developing reforms.

Clubs Australia supports a risk-based approach for FRT, including adequate consideration of human rights and assessment of the use of FRT. We also consider that the settings and controls underpinning the use of the technology be proportionate.

Privacy impact assessments for high-risk activities

The Review Report recommends that every business using FRT conduct a privacy impact assessment (PIA). Requiring every club to conduct a PIA would be unnecessarily burdensome, given the similar circumstances and risk profiles between the businesses who intend to use FRT to administer gambling self-exclusions.

Clubs Australia instead recommends consideration be given to PIAs being completed on behalf of an industry, where the use of the technology involves similar circumstances and risk profiles between the businesses. Under such an approach, businesses whose circumstances differ materially would be required to conduct another assessment to supplement the industry-wide PIA, to address additional risks.

Clubs Australia recommends privacy impact assessments for FRT be capable of being conducted on behalf of an industry, where the circumstances and risk profiles are similar.

Right to Erasure

Clubs Australia supports the intention behind introducing of right for individuals to erase their personal information, however, we are concerned about potential unintended consequences.

Self-Exclusions

As noted earlier, clubs across Australia have self-exclusion programs that allow an individual to exclude themselves venues to stop them from gambling.

In many states and territories, self-exclusions require the patron to complete and sign a self-exclusion deed. These deeds require the collection of personal information necessary to ensure venues can enforce the exclusion. These deeds are legally enforceable and are a key tool to assist people who may be experiencing problems with gambling.

Clubs Australia believes that a self-exclusion deed would fall under the 'relationships with a legal character' exemption to all rights of the individual. Clubs Australia would be concerned if this was deemed not to be the case as, in practice, this may lead to patrons requiring clubs to erase all their personal information and it would then become practically impossible to enforce the self-exclusion.

Constitutional Disciplinary Process

Club members are bound by the governing rules of the Club, which include the Club's Constitution and By-Laws. When a person applies for a club membership, the terms and conditions will often bind the applicant to the club's constitution and any other rules (such as by-laws) that are enforced. The club constitution is deemed to be a contract under corporations law.

An important process in a club's constitution is the 'disciplinary process', which enables the board of a club to reprimand or suspend any or all of a patron's privileges of membership for a period they see fit.

To be able to effectively manage the suspension of a member, clubs need to be able to keep the personal information of a suspended member to ensure the member does not enter or utilise any of the club's facilities. If a suspended member could request the erasure of their personal information, this would make the enforcement of a suspension nearly impossible for clubs. Clubs Australia believes in this instance that the relevant exemption to the right of the individual would be a technical exemption, as it would be unreasonable for the club to comply with this request.

Clubs Australia supports exemptions to right for individuals to seek erasure of their personal information, to ensure clubs can continue to meet their business and harm minimisation requirements.

Industry Funding Model

Clubs primarily collect, use, and disclose personal information in accordance with their legislative obligations, and otherwise use personal information in a manner ancillary to their principal hospitality activities. The primary use of personal data by clubs is to maintain an accurate list of members, and to ensure that those members receive appropriate notice of club elections and meetings. While clubs may use personal information to email or text members promotional materials, neither the collection, use or disclosure of personal information is central to the business model or revenue-generating activities.

Applying privacy laws to clubs ultimately supports clubs in adopting suitable privacy practices, which is an avenue to ensure individual privacy is protected.

Given that the goal of the Privacy Act is focused on individual protection, Clubs Australia does not consider that businesses should contribute to these costs.

An additional levy on clubs would cause a significant financial burden.

Clubs Australia believes that any industry funding model should exclude businesses that do not commercialise or profit from personal information.

Contact information

Clubs Australia is grateful for the opportunity to comment on the Government's Response to the Privacy Act Review Report. Should you wish to discuss this submission further, please contact Simon Sawday, Executive Manager of Policy and Government, on 02 9268 3028 or ssawday@clubsaustralia.com.au.