Clubs Australia

Regulatory Intelligence and Strategy Branch
Office of the Australian Information Commissioner

Dear Shona Watson

**Re: OAIC AML/CTF Privacy Guidance – Consultation Draft (September 2025)**

Clubs Australia welcomes the opportunity to provide feedback on the draft guidance jointly released by the Office of the Australian Information Commissioner (OAIC) and AUSTRAC regarding the interaction between the Privacy Act 1988 and the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act).

Clubs Australia represents over 5,000 not-for-profit licensed clubs across the country which directly employ more than 140,000 people. All clubs are community-based, member-owned and many are small businesses operating in regional or rural areas. Clubs with gaming machines are already reporting entities under the AML/CTF Act and have long navigated the intersection between privacy and AML/CTF obligations.

This consultation represents the first time that the OAIC has provided sector-neutral guidance on how the Privacy Act applies in the AML/CTF context. We appreciate this initiative and support the intent of embedding stronger privacy practices. We particularly value how clear and easy to follow the draft guidance is — this accessibility will make it far more useful to entities in practice. We submit that the draft guidance could be further developed to ensure it is practical, proportionate, and tailored to the realities of existing reporting entities like clubs.

**Summary of recommendations**
To ensure the guidance is useful for existing entities such as clubs, we believe four changes are critical:

- **Expand Case Studies to Tranche 1 and Club Entities**

The draft is largely targeted at tranche 2 businesses that will only enter the AML/CTF framework from 2026. Existing tranche 1 entities such as clubs are already subject to extensive AML/CTF obligations but are not referenced in the draft. Adding case studies that reflect real-world club operations will benefit the guidance improving practicality, accessibility and ease of implementation. A case study for clubs that are under $3 million in annual turnover and fall under the Privacy Act solely because of AML/CTF, would also be of benefit.

- **Clarifying Privacy and AML Intersections**

While AUSTRAC requires clubs to retain records for seven years — which should satisfy APP 11 — the draft guidance does not make this explicit. OAIC should confirm that retention

Clubs Australia Incorporated
ABN 32 691 361 915

Level 8, 51 Druitt Street
Sydney NSW 2000
P 02 9268 3000 F 02 9268 3066

in line with AUSTRAC's obligations, including any information reasonably considered necessary, will be regarded as consistent with APP 11. This clarity would reduce over-collection and give clubs confidence their policies meet both regimes.

- **Publishing Practical Toolkits and Resources**

The guidance should be accompanied by practical tools, such as topic/APP specific checklists, a simplified "AML/CTF-only" checklist for small clubs, and a model privacy notice pack (including signage and staff scripts), to help entities apply the principles in practice. OAIC has used this approach effectively in other areas (e.g. privacy management plan templates, data breach response flowcharts). Providing a tailored toolkit alongside the guidance will materially lift compliance outcomes for small clubs and ensure that privacy and AML/CTF obligations are implemented consistently and proportionately.

- **Addressing Biometrics as a Key Emerging Issue**

Biometric tools such as facial recognition are increasingly considered by clubs to strengthen AML/CTF compliance, but the legal boundaries remain unclear. The guidance should specifically address the use of facial recognition for mitigating and managing AML/CTF risk, including the factors OAIC would consider in assessing compliance with the Privacy Act. This should cover when collection is "authorised by law," the minimum safeguards expected (e.g. proportionality, secure storage, access controls, staff training), and practical examples of proportionate use (such as large payouts or repeat monitoring of high-risk patrons). Clear direction would help clubs adopt these technologies responsibly while giving patrons confidence that sensitive data is protected.

In addition to these critical reforms, Clubs Australia recommends the OAIC further strengthen the guidance by:

- Developing a model privacy notice that can be incorporated into club membership and CDD processes; and
- Clarifying the treatment of third-party vendors: Provide guidance on how APP 6 applies when clubs engage AML/CTF service providers, including when provision of information will be a disclosure versus a use (for agent-style arrangements), and outline the core safeguards OAIC expects in vendor agreements (purpose limitation, confidentiality, security, breach notification, sub-processor controls, data location/transfer).

For further information, please contact Alex Staric [redacted]

## A. Relevant Case Studies and Tailored Examples

Clubs Australia welcomes the intent of the OAIC guidance but notes that it is heavily framed around tranche 2 businesses. Existing tranche 1 entities such as clubs, which have long been reporting entities under the AML/CTF Act, are not adequately represented.

Although clubs have applied AML/CTF obligations for many years, we have not previously received this level of privacy-focused guidance. The opportunity to embed privacy considerations into established AML/CTF processes is welcome and would be particularly helpful to our industry if tailored examples are provided.

This need is especially pressing for small clubs with turnover under $3 million, which are otherwise exempt from the Privacy Act but fall within its scope solely because of AML/CTF obligations. Around 80% of clubs nationally fall below this threshold. These are not-for-profit, community-based venues — often volunteer-run or staffed by people wearing multiple hats across governance, operations, and compliance. For this cohort, tailored case studies would not only provide proportionality but also serve as the most practical way to demonstrate how privacy principles apply when AML/CTF obligations are the only driver of Privacy Act exposure.

Unlike tranche 2 entities such as lawyers, accountants, conveyancers, or real estate agents, clubs do not operate on the basis of structured, appointment-based client relationships. Clubs are high-volume, community venues where members and visitors can access designated services in a walk-in environment, often without clear indicators at the point of entry. This makes it far more complex to determine in advance when and how to apply AML/CTF obligations, and it underlines the importance of case studies that demonstrate how privacy principles should work in practice in this setting.

The following practical issues justify the need for tailored case studies:

- **Operational Relevance**: Clubs already hold extensive membership data and have AML/CTF controls in place. A case study illustrating how the APPs apply to existing designated services (gaming, payouts) would immediately anchor the guidance in lived experience.
- **Small Business Complexity**: A case study showing a small club under $3m turnover navigating privacy obligations solely for AML purposes would highlight the proportionality issues and assist other small reporting entities.
- **Cross-Sector Consistency**: Without tranche 1 examples, the document risks creating the impression that privacy obligations apply only to tranche 2 entities, when in fact they apply to all reporting entities including clubs.

**Clubs Australia Recommendation**

Clubs Australia recommends that the OAIC expand the draft guidance to include case studies for tranche 1 entities, specifically clubs, and develop a specific example for registered clubs under the $3m threshold. This will ensure the guidance is relevant to existing reporting

entities, promote proportionality for small businesses, and avoid duplication across privacy and AML frameworks.

To make this tangible, OAIC could:

- Include a case study in Chapter 3 (Collection of personal information) demonstrating how APP 3 applies in a walk-in venue such as a club.
- Include a case study in the Small Business section on a club under $3m turnover that only has Privacy Act obligations because of AML/CTF.

## B. Clarifying Privacy and AML Intersections

The draft guidance highlights APP 11 obligations to destroy or de-identify personal information when it is no longer needed. At the same time, the AML/CTF Act requires reporting entities to retain customer due diligence (CDD) and transaction records for seven years.

In principle, retaining records to meet a clear legislative requirement should satisfy the "reasonably necessary" test under APP 11. However, the absence of an explicit statement in the guidance leaves uncertainty for clubs when designing retention and deletion policies. Out of an abundance of caution, many venues may over-collect or hold additional information "just in case," which increases risk without improving compliance outcomes.

The following realities demonstrate why clear direction is essential:

- **Mandatory Retention**: Clubs are legally required to hold AML/CTF records for seven years. Destroying them earlier would expose them to potential enforcement action by AUSTRAC.
- **Operational Ambiguity**: While the Privacy Act is principles-based, the concept of when information is "no longer needed" leaves room for interpretation. Without clear direction, clubs are left uncertain about how APP 11 should interact with the prescriptive seven-year retention requirements of the AML/CTF framework.
- **Cyber Security Risks**: Clubs are told simultaneously to minimise data holdings while also retaining large volumes of sensitive data for long periods due to legislative obligations This contradiction increases the risk surface for data breaches.

*Data minimisation in practice*

While AUSTRAC sets the record-keeping requirements, the guidance could help clarify if a club retains all information they reasonably believe is required to meet AUSTRAC's obligations, this will be regarded as consistent with APP 11. Explicit confirmation from OAIC would reduce uncertainty and give clubs confidence to design proportionate record-keeping policies.

*Access and Correction Limitations (APP 12/13)*

The guidance should also recognise that individuals' rights under APP 12 (access) and APP 13 (correction) are subject to legal restrictions in the AML/CTF Act (including suspicious matter

reporting and tipping-off prohibitions). Clubs should not disclose or confirm the existence of records if doing so, would breach those prohibitions; instead, they should be able to provide a lawful, general explanation and refer individuals to their Privacy Policy.

**Clubs Australia Recommendation**
Clubs Australia recommends that the OAIC strengthen the APP 11 section of the final guidance by clarifying how AML/CTF record-keeping obligations interact with privacy requirements. Specifically, the guidance should:

- Confirm that retention of AML/CTF records for seven years, as required by AUSTRAC, will be considered compliant with APP 11.
  *Suggested drafting for inclusion:*
  *"Where an entity retains customer due diligence and transaction records in accordance with the AML/CTF Act's seven-year requirement, this will be regarded as compliant with APP 11."*
- Clarify that that retention of any information an entity reasonably considers necessary to meet AUSTRAC's obligations will be regarded as compliant with APP 11.
- Confirm in the APP 12/13 sections that access and correction rights are subject to AML/CTF tipping-off restrictions. Clubs should not disclose or confirm the existence of certain records, if doing so would breach the AML/CTF Act; a general explanation and reference to the Privacy Policy should be considered sufficient.

## C. Practical Tools and Templates for Compliance

The draft guidance is comprehensive but principle heavy. For small and regional clubs, compliance is rarely handled by a dedicated team; staff often wear multiple hats across governance, operations, and compliance, and many venues rely heavily on volunteers. Ready-to-use tools would support implementation and make it more consistent across the industry.

Compliance outcomes would be materially strengthened if the OAIC and AUSTRAC paired the guidance with checklists, templates, and flowcharts that translate principles into clear, accessible actions. This approach is consistent with what has worked in other regulatory settings (e.g. WHS, liquor licensing), where practical aids have supported small community businesses to meet their obligations with confidence. The club industry is familiar with this style of support, which has proven effective in helping venues understand and comply with their obligations.

The OAIC has itself demonstrated the value of these tools in other areas, including its APP privacy policy guidance, data breach response flowcharts, and Privacy Foundations self-assessment tool.

For clubs, such tools would address the following challenges:

- **Resource Constraints**: Many clubs lack in-house privacy expertise and depend on volunteers or part-time compliance officers.

- **Duplication with Other Laws**: Clubs already collect and store information under the Corporations Act and other jurisdictional legislation. Without clear tools, duplication and confusion are inevitable.
- **Notice Requirements**: APP 5 notices are impractical to deliver at every customer touchpoint in a high-volume environment. A model "AML Privacy Notice" template endorsed by OAIC/AUSTRAC would enable consistent, transparent disclosure without excessive burden.

Clubs understand AML/CTF's risk-based nature and do not propose a copy-and-paste approach. Templates and checklists help operators apply the guidance to their risks (e.g., tailoring fields, triggers, and retention rules), rather than substituting for judgment.

**Clubs Australia Recommendation**

Clubs Australia recommends OAIC and AUSTRAC jointly develop, alongside the final guidance, the following resources:

- Implementation Checklists – topic-by-topic checklists covering collection, notices, permitted disclosures, access/correction, security, and retention/deletion; plus, a simplified "AML-only" checklist for small clubs whose Privacy Act exposure exists solely due to AML/CTF.
- Privacy Notice Pack – a model APP 5 collection notice, venue signage ("why we collect" + tipping-off caveat), and staff scripts for payout/jackpot scenarios.
- Retention & Deletion Decision Aid – a simple reference mapping AML/CTF record types to the seven-year requirement, clarifying when APP 11 deletion/de-identification applies afterwards.
- Frontline Flowchart – a one-page flowchart showing the AML/CTF privacy journey (identify designated service → collect/verify → notify (if appropriate) → record → secure → retain/delete).

Additionally, Clubs Australia suggests that OAIC include an annex with sample wording for an APP 5 AML privacy notice. For example:

*"We collect personal information from you to meet our obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006. If we cannot collect this information, we may not be able to provide certain designated services. For more information, please see our Privacy Policy."*

Providing such a model would give clubs a clear starting point, while still allowing them to adapt the language to their size, services, and risk profile.

## D. Sensitive Information and Biometrics

Clubs are increasingly required to handle sensitive personal information as part of AML/CTF compliance. A growing number of venues are considering biometric solutions — such as facial recognition — to strengthen identification, support sanctions/PEP screening, and assist in monitoring higher-risk transactions. These technologies have real potential to improve compliance outcomes, but they also heighten privacy risks given the sensitivity of biometric data under the Privacy Act.

Clubs operate in fast-paced, walk-in environments where patrons can access designated services without advance notice. This creates practical challenges for monitoring and verification, particularly where the same individual may engage in multiple activities across a venue. Biometric tools can help address these gaps — for instance, by confirming that a person claiming a payout is the one who played the gaming machine, recognising repeat visits for transaction monitoring, or applying additional checks only in higher-risk scenarios such as large cash payouts.

From a sector perspective, biometrics are a natural next step in strengthening compliance, but the absence of clear expectations creates uncertainty. Clubs want to adopt these tools responsibly but do not know the legal boundaries. Without clarity, venues may either avoid innovation — missing opportunities to improve compliance — or adopt systems that later prove non-compliant. Clear OAIC guidance would therefore support both clubs and patrons by enabling proportionate systems that meet AML/CTF obligations while giving members confidence that sensitive data is handled lawfully and responsibly.

Clubs face uncertainty about:

- Whether biometric collection for AML/CTF compliance purposes is considered “authorised by law” under APP 3.4(a) and/ or whether OAIC also sees scope for it to be supported in some cases by a permitted general situation under s16A of the *Privacy Act*.
- What safeguards (e.g. proportionality, storage limitations, role-based access controls, staff training) are expected to meet Privacy Act standards; and
- Whether OAIC supports risk-based or limited application (e.g. biometrics for large payouts or repeated high-risk patrons, rather than universal entry).

As part of addressing these safeguards, OAIC could also encourage entities to undertake a proportionate Privacy Impact Assessment (PIA) before deploying biometric tools. This would align with OAIC’s existing approach to high-risk data handling, and mirrors international best practice — for example, the UK Information Commissioner’s Office (ICO) and the Office of the Privacy Commissioner of Canada (OPC) both recommend impact assessments when organisations implement facial recognition or other biometric technologies.

**Clubs Australia Recommendation**

Clubs Australia recommends that the OAIC treat biometrics as a key area in the final guidance. Specifically, the guidance should:

- State that biometric information collected for the purpose of managing and mitigating ML/TF risk in accordance with the AML/CTF Act and Rules may be treated as authorised either under APP 3.4(a) (authorised by law) and/or under the permitted general situations in s16A of the *Privacy Act*, provided the collection is reasonably necessary and proportionately safeguarded.
- Outline the minimum safeguards expected when using biometrics (e.g. proportionality, strict access controls, secure storage, audit trails, staff training, and retention/deletion rules) and encourage entities to undertake a proportionate Privacy Impact Assessment (PIA) before deployment.
- Provide practical examples of when biometric use is proportionate (such as high-value payouts, sanctions/PEP screening, or repeated monitoring of identified high-risk patrons).
- Confirm that entities should provide clear notice about why biometric information is being collected and how it will be protected, using signage, membership forms, or digital notices. A model notice could include wording such as: "*This venue may use facial recognition for AML/CTF compliance (e.g., to verify identity during payouts). Images are stored securely and only used for compliance purposes."*

## E. Clarification of Industry-Specific Issues

There remain several practical uncertainties for clubs where clearer privacy guidance would significantly reduce compliance risk. While we recognise that AUSTRAC is the lead agency on AML/CTF program design, there are privacy intersections where the OAIC's perspective is essential.

- **Scope of Screening:** Clubs need clarity on how APP 3 ("reasonably necessary" collection) interacts with sanctions/PEP screening. The timing of information capture is inconsistent across clubs — some patrons swipe a membership card at entry, others present ID at reception or use digital membership, and in some cases sign-in only occurs later when accessing a designated service. These differences directly affect when personal information is available for sanctions/PEP screening, creating uncertainty as to whether clubs may collect and screen information universally at entry, or only once a designated service is accessed. OAIC guidance on what is "reasonably necessary" in this scenario would provide clubs with greater confidence.
- **Visitor Identification:** Under AUSTRAC's risk-based approach, visitors are often classified as low risk when entering a club (e.g. dining or attending an event), so only minimal information is collected at entry. If the same visitor later accesses a designated service (such as gaming or requesting a payout), more detailed AML/CTF checks are required. This staged process creates uncertainty about how APP 3 ("reasonably necessary" collection) and APP 5 (notification) apply in practice. OAIC guidance could clarify that where advance notification is impracticable, it is acceptable to collect and notify "as soon as practicable" once the designated service is accessed, and that venue signage or other general notices can be used to meet APP 5 obligations in these high-volume environments.

- **Third-Party Providers (APP 6 Use/Disclosure):** Clubs rely on third-party vendors — such as sanctions/PEP screening providers and membership/ID system vendors — to perform AML/CTF functions. The guidance could assist in clarifying whether providing personal information to such vendors is considered a "use" by the club (where the provider acts under the club's instructions as its agent) or a "disclosure" to a separate entity.

**Clubs Australia Recommendation**

Clubs Australia recommends the OAIC address the following issues directly in the guidance, with suggested practical insertions as set out below:

- **Clarifying CDD information collection under APP 3**: Insert a note in the Collection (APP 3) chapter clarifying that "reasonably necessary" collection must be interpreted in light of AML/CTF customer due diligence (CDD) obligations, as well as PEP/sanctions screening
- **Clarifying visitor notification under APP 5**: Insert an example in the Notices (APP 5) confirming that staged notification is acceptable in a risk-based AML/CTF environment. For instance:

  "*In a walk-in venue such as a club, where it is not practicable to notify a visitor before information is collected for AML/CTF purposes, notification should occur as soon as practicable afterwards — for example, through general venue signage at entry and/or a membership form when the patron later accesses a designated service*.
- **Clarifying treatment of third-party vendors under APP 6**: Confirm that engaging a third-party provider to deliver AML/CTF functions (such as sanctions/PEP screening or membership/ID systems) will ordinarily be considered a "disclosure" of personal information by the club, rather than a "use".
- **Outlining expected safeguards in vendor agreements**: Direct entities to ensure vendor agreements contain clear privacy and security protections, with OAIC outlining the key categories expected (e.g. purpose limitation, confidentiality, security, and breach notification).