COMS DETECT PRIVACY STATEMENT

1. SUMMARY

What this policy covers: We collect and use facial recognition and related personal information to help venue operators identify excluded or banned individuals, minimise harm (at-risk persons) and support banned-member management

We treat all personal and sensitive information carefully, and this policy explains how we do that – what we collect, how we use and disclose it, your rights, and how you can contact us.

For full details, please refer to the full version of the policy below.

2. FULL PRIVACY POLICY

2.1. SCOPE

This policy applies to:

- The mobile/web application and associated services (the "App") provided by COMS Systems Limited ("we","us","our"), in association with client venues (our "Clients").
- The processing of **personal information** collected or uploaded to the App, including facial imagery, biometric templates, identity verification data, consumer details, patron status (excluded, banned, at-risk), alerts and logs.
- Use in Australia by the Client at their venues (including but not limited to licensed premises, hotels, clubs, casinos).
- All users of the App (including venue staff, security personnel), and any individuals whose images or data are processed (which may include patrons, excluded persons, banned persons, a-risk persons and other visitors).

2.2. WHAT KINDS OF PERSONAL INFORMATION WE COLLECT

We collect, hold and use the following types of information:

- Facial images of individuals captured at venue access points or monitoring zones.
- Biometric templates derived from face imagery (for matching purposes) – this is sensitive personal information.
- Identify verification data such as name, date of birth/age, photograph, membership or exclusions status.
- Patron-status information: e.g., whether an individual is excluded, banned, under harm-minimisation supervision, or at-risk.
- Timestamps, location of capture (venue identity/location), entry/exit logs.
- Device identifiers and audit logs of App usage by venue staff.
- Where relevant, incident/alert data (e.g., when a match is made, what action was taken) and disclosure logs.
- (Optional) If your venue adds ancillary data: e.g., membership records, misconduct records, CCTV logs, etc.

We treat biometric and sensitive personal information with high care.

2.3. HOW WE COLLECT PERSONAL INFORMATION

We collect information in the following ways:

- Directly at the venue: an individual enters the premises and is captured by the facial recognition system (with notice).
- From the venue's lists: the venue provides excluded, banned or at-risk person lists which we integrate with.
- From the App usage: the staff capture or trigger scans using the App, upload imagery or data to our system.
- Automatically: via the App or monitoring system, capturing still images, logging date and time, location, and device tag.

- From third parties: e.g., regulatory bodies, venue management systems, membership or exclusion databases (with lawful basis).

We only collect information that is necessary for the purpose described in section 2.4

2.4. PURPOSE OF COLLECTION, USE AND DISCLOSURE

Purpose of collection and use:

- To enable venue staff to identify excluded, banned, or at-risk persons upon entry or within the venue.
- To support harm-minimisation efforts (identifying persons at risk of harm or whose behaviour is of concern).
- To log incidents, provide alerting and audit trails for compliance, regulatory or safety purposes.
- To enable reporting to clients on matched events, usage statistics, system performance and compliance.
- To maintain and update patron-status records (excluded, banned, at-risk) and to manage access control effectively.
- To manage our system operations: security, auditing, analytics (non-identifying where possible), and improvement of the App.

We may disclose personal information:

- To the Client venue, when the system makes a match or alert regarding an individual.
- To any contracted service providers (e.g., cloud-hosting, biometric matching engine, support) who require access under strict confidentiality and security obligations.
- To regulatory or law-enforcement authorities if required by law, or in cases of serious threat/harm or suspected illegal activity.
- To overseas recipients? **No** - we do **not** routinely disclose personal information to overseas entities. If this changes, we will update the policy and advise affected individuals.
- We do **not** sell personal information to third parties for marketing purposes.

2.5. HOLDING AND SECURITY OF PERSONAL INFORMATION

- We hold personal information in encrypted form, both at rest and in transit, on secure servers/cloud infrastructure.
- Access to biometric templates and image data is strictly limited to authorised personnel and subject to logging and audit.
- Venue staff access via the App is role-based, with unique credentials, multi-factor authentication (where enabled) and periodic review of access rights.
- We maintain incident response procedures for data breaches, and will comply with the Notifiable Data Breaches scheme under the Privacy Act 1988.
- We keep logs of who accessed, modified, or disclosed data, and conduct regular security risk-assessments in line with the OAIC information-security guidance.
- We retain personal information only as long as necessary for the purpose for which it was collected, and will securely destroy or de-identify it once no longer required (e.g., after a defined retention period set by the Client and/or under regulatory obligations).

2.6. ACCESS AND CORRECTION

- Individuals may request access to their personal information held within our system, or request correction of inaccurate or out-of-date information.
- To make such a request, please contact us (see section 2.9) and provide sufficient detail to identify yourself and the information sought.
- We will respond within a reasonable period (as required by the APPs).
- If we deny access or correction, we will provide the reasons for denial (unless legally prohibited).
- If you believe that our information about you is incorrect (for example, a “match” alert was incorrect), you may request correction and we will take steps to verify and correct the record, or mark it as disputed if necessary.

2.7. COMPLAINTS

- If you believe we have breached the APPs, this privacy policy, or your privacy rights, you may lodge a complaint with us.
- We will respond to your complaint promptly (within a specified timeframe) and keep you informed of progress.
- If you are dissatisfied with our response, you may refer the matter to the OAIC: www.oaic.gov.au or 1300 363 992.

2.8. OVERSEAS DISCLOSURE

As noted above, we **do not** routinely send personal information to overseas recipients. If we do so in future, we will clearly identify likely countries and require your informed consent or provide an opt-out mechanism.

2.9. CONTACT DETAILS

For any questions about this privacy policy, to request access/correction, or to lodge a complaint, please contact:

COMS Systems Limited

Email: complaints@coms.services

Phone: 1800 324 918

2.10. CHANGES TO OUR POLICY

We may update this policy from time to time (e.g., when our App functionality changes). We will publish the revised version on our website and notify Clients. The latest version always applies.

3. ADDITIONAL CUSTOMISED CLAUSES FOR FACIAL RECOGNITION / HARM-MINIMISATION

Because the App uses facial recognition technologies and processes sensitive biometric information, the following additional provisions apply:

3.1. BIOMETRIC/FACE-RECOGNITION PROCESSING

- Our system uses face-capture and biometric matching to identify individuals who are on excluded, banned or at-risk lists supplied by the Client.
- Where face imagery or biometric templates are created, held and matched, this constitutes "sensitive information" under the Privacy Act. We only process this where it is reasonably necessary for the purpose of identifying excluded, banned or at-risk persons in a venue environment.
- Venue signage and patron notice: the Client must ensure visible signage (or other notice) at access points to the venue that facial recognition is in use, how the data is processed, and contact details for queries (our contact or the venue's).
- Accuracy/human-oversight: alerts from the system are subject to human review by venue staff before action is taken (e.g., exclusion enforcement or harm-minimisation support).
- Data minimisation: only image/biometric data necessary for match-purposes is stored; we do not store full imagery beyond what is needed for the matching process (or we store only encrypted templates, as per Client's configuration).
- Retention/deletion: Matched-events records (including image captures and audit logs) are retained for the duration of the membership or exclusion period and consistent with applicable laws/regulations; after that period, they are securely destroyed or de-identified.
- Risk-management: We have undertaken a Privacy Impact Assessment (PIA) for biometric processing, considered the risks (mis-identification, bias, unauthorised access), and put in place safeguards (encryption, access logs, independent audit).
- Vulnerable persons: Where at-risk persons (e.g., persons with impaired decision-making capacity) are involved, venue staff must follow additional harm-minimisation protocols, ensure safe-space response and liaise with appropriate welfare services as required.
- Training and audit: Venue staff using the system must be trained in responsible use and privacy obligations (including not misusing matches), and we conduct periodic audits of system usage for compliance and proper use.

3.2. MEMBERSHIP/EXCLUDED/BANNED PERSONS LIST MANAGEMENT

- The Client is responsible for supplying, updating and maintaining accurate membership/excluded/banned/at-risk lists in compliance with relevant legislation and licensing conditions.
- We process the list strictly for the approved purpose of match-detection at venue access. The list is securely transmitted and stored in encrypted form.
- When a person is matched, an alert is generated for venue staff; the subsequent action (e.g., denial of entry, safe removal) is the Client's responsibility, and this policy does not govern the operational decision-making beyond data handling.
- We log all matches, including date, time, venue, staff user, match confidence, follow-up action (if recorded) - these logs are available to the Client for audit/compliance purposes.

3.3. AT-RISK PERSONS/HARM-MINIMISATION

- The system may be used to flag individuals identified by the venue as at-risk (for example based on intoxication, previous incidents, self-harm potential).
- Match to at-risk persons triggers alerts to venue staff and may prompt tailored responses (e.g., welfare check, escort, referral to support). The processing of at-risk person data is subject to heightened sensitivity.
- Where possible, the venue should ensure patron consent (within the license/venue policies) and clear provision of notice about how the system works, what happens if a match occurs, and how data will be handled.
- The system is **not** used for general biometric profiling of all patrons beyond the scope of membership/excluded/banned/at-risk. Blanket collection beyond the necessary purpose is not permitted.

3.4. DISCLOSURE TO THIRD PARTIES

- If we engage third-party service providers (such as cloud hosting, biometric algorithm providers, support contractors), they are bound by our contractual privacy, security and confidentiality obligations.
- If the Client wishes to share match-information with law enforcement or regulatory bodies, that is the Client's decision; we will support secure transmission if required by law or regulatory request.

4. CLIENT RESPONSIBILITIES

As the venue or Client using our App, you are responsible for:

- Ensuring patrons are made aware of the facial-recognition system via signage or other mechanisms ("This venue uses facial-recognition technology. By entering you consent to your image being captured and processed for the purposes of excluded, banned and at-risk patron detection.")
- Supplying and keeping accurate lists of excluded, banned and at-risk persons in the agreed format and updating them promptly when status changes.
- Ensuring venue staff are properly trained in the use of the App, match-response protocols, harm-minimisation procedures and access to data/information.
- Ensuring that any follow-up actions (e.g., refusal of entry, safe removal, welfare checks) comply with relevant legislation, licensing conditions, harm-minimisation requirements and that data-handling flows are consistent with this policy.
- Providing patrons with a copy (or link) to this privacy policy (or summary) and responding to patron queries about how their data is handled.
- Cooperating with audits or reviews of system use, match-logs and data-handling practices, when requested.

5. RETENTION AND DE-IDENTIFICATION POLICY

- We retain biometric templates, match-logs, and image captures linked/matched with membership or exclusion lists, for the duration of the membership or exclusion period and in compliance with applicable legislation.
- We retain biometric templates, match-logs, and image captures **not** linked/matched with membership or exclusion lists, for 72 hours and in compliance with applicable legislation.
- After the retention period expires, we delete or irreversibly de-identify the information (for example, by destroying the biometric template and image data so it can no longer identify an individual).
- We may retain aggregated, non-identifying statistical data (e.g., number of matches per month, system usage metrics) indefinitely for analytics, improvement and compliance reporting.

6. DATA BREACH AND INCIDENT RESPONSE

- In the event of an eligible data breach (unauthorised access, disclosure or loss of personal or biometric data), we will follow our incident response plan and notify affected individuals and the OAIC as required under the Notifiable Data Breaches scheme in the Privacy Act.
- We will also inform the Client venue without undue delay so that coordinated response can occur (e.g., patron notification, regulatory filings, mitigation).
- We conduct periodic security reviews and audits of the system, access logs and use of the App to detect misuse or inappropriate access.

7. YOUR RIGHTS AND CHOICES

You have the following rights:

- You may access the personal information we hold about you and request correction if it is inaccurate or out-of-date.

- You may request a copy of the list (if you are on it) or request removal/correction of your data (subject to legal/regulatory requirements).
- You can decline or withdraw consent (to the extent applicable) - for example by refusing to enter the venue or not participating; however, you should note that if you are on an excluded/banned list, venue entry may be refused.
- You can ask questions or make a complaint if you believe your privacy has been breached (see section 2.7).
- You can request our policy in an alternate format (see OAIC APP 1.6).

We will not discriminate or penalise you for exercising your rights.

8. GLOSSARY AND DEFINITIONS

- **Excluded person**: an individual who is not permitted entry to the venue under the venue's or regulatory body's policy.
- **Banned person**: an individual formally banned by the venue or regulatory body from access.
- **At-risk person**: an individual identified by the venue (or regulatory body) as requiring additional safety/harm-minimisation measures (for example because of intoxication, behavioural risk, self-harm risk).
- **Biometric template**: a mathematical representation derived from facial imagery used for matching; it does not necessarily allow the reconstruction of the full image.
- **Face-matching**: The process by which the captured face data is compared against the stored templates to determine if a person in the venue matches an excluded, banned or at-risk individual.
- **Client**: the venue, club or operator using our App and supplying the patron-status lists.
- **We/Us/Our**: COMS Systems Limited, the provider of the App and associated biometric/matching service.

9. POLICY REVIEW AND VERSION CONTROL

This policy is Version 1.0, Ref: 3078029319, dated 21 November 2025. We will review it at least annually or sooner if our systems, processing or legal/regulatory environment changes. Clients will be notified of material changes (including via update notices in the App or by direct email).