# WATCHGUARD PRIVACY STATEMENT

## 1. SUMMARY

**What this policy covers:** We collect and use facial recognition and related personal information to help Clients identify individuals enrolled in the system for approved operational purposes, including VIP patrons or loyalty programme members (where applicable and consent given), and individuals subject to access restrictions (such as trespass, exclusion or bans) and support safety and security processes, and manage related alerts, records, and system activity.

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 WatchGuard mobile/web application and associated services (the "App"), operated under the "WatchGuard by COMS" brand and provided by COMS Systems Limited ("we","us","our"), in association with our client (our "Clients").
- The processing of **personal information** collected or uploaded to the App, including facial imagery, information derived from biometric processing, identity verification data, individual-related information, individual status (trespassed, excluded, banned, flagged for safety or security), alerts and logs.
- Use in **New Zealand** by Clients within their business operations, including (but not limited to) retail and service environments.
- All users of the App (including staff and security personnel), and any individuals whose images or data are processed through the App including patrons, visitors, individuals

enrolled for approved operational purposes, and individuals subject to access restrictions ( such as trespassed, excluded or banned), or otherwise assessed as presenting a safety or security risk in accordance with Client policies and applicable New Zealand laws.

## 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 entry points, monitoring zones, or other locations where the App is deployed.
- Identity verification data such as name, date of birth/age, photograph, membership information, and exclusion-related information.
- Status information consisting of information about an individual's enrolled status within the App, such as VIP, loyalty member, trespassed, excluded, banned, or other client-defined operational, safety, or security designations.
- Timestamps, location of capture (business identity/location), entry/exit logs.
- Derived or inferred information generated through system processing (such as estimated age ranges or similar attributes), where used for safety, compliance, or approved operational purposes.
- Device identifiers and audit logs of App usage by staff and security personnel.
- Where relevant, incident/alert data (e.g., when a match is made, what action was taken) and disclosure logs.
- (Optional) Additional information added by Clients: e.g., notes, membership records, misconduct records, CCTV logs, etc.

We treat biometric and sensitive personal information with high care and in accordance with applicable laws.

## 2.3. HOW WE COLLECT PERSONAL INFORMATION

We collect information in the following ways:

- Directly at Client locations: an individual enters the premises and is captured by the facial recognition system (with notice).
- From the Client-provided data: Clients may provide information about individuals enrolled in the App, including VIP or loyalty programme members (where applicable and consent given), and individuals who have been designated by the Client as trespassed, excluded, banned, or otherwise subject to a Client-defined operational, safety, or security designation.
- From the App usage: authorised staff capture images using the App, which are uploaded to our system.
- Automatically: via the App or monitoring system, capturing still images, logging date and time, location, and system-derived attributes.
- From third parties: e.g., regulatory bodies, Client management systems, membership or exclusion databases (with a 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 Client staff and authorised personnel to identify individuals enrolled in the App for approved operational purposes, including VIP patrons or loyalty programme members (where applicable and consent given), and individuals subject to access restrictions such as trespassed, excluded or banned.
- To support safety, security, and harm-prevention measures through the identification of individuals who have been designated by the Client for operational, safety or security purposes.

- To support safety, compliance, and operational measures through the use of system-generated insights (such as age estimation or similar analytics), where reasonably necessary and proportionate to the purpose.
- To record and manage incidents, generate alerts, and maintain audit trails for safety, compliance, and regulatory purposes.
- To provide reporting to Clients on system activity, including matched events, anonymous usage statistics, system performance, and compliance-related insights.
- To maintain and update individual records and status information within the App, including enrolment categories, access restrictions and other Client-defined operational, safety or security designations.
- To manage and maintain the security, integrity, and performance of our systems, including auditing, analytics (using non-identifying data where practicable), and ongoing improvement of the App.

We may disclose personal information:

- To Clients, where the system generates a match, alert, or relevant information relating to an individual.
- To any contracted service providers (e.g., cloud-hosting, biometric matching engine, support) who require access under strict confidentiality and security obligations.
- Through a centralised system:
    - Within Client operations, where information (such as trespassed, excluded or banned status) is shared across multiple locations or related entities operated by the same Client.
    - Across participating Clients, where information relating to individuals subject to access restrictions or other approved safety and security designations is shared as part of local, regional, or national safety and security programmes or databases, where those Clients have agreed to participate and such sharing is carried out in accordance with applicable laws and appropriate safeguards.
- To regulatory or law enforcement authorities if required by law, or in cases of serious threat/harm or suspected illegal activity.

- To overseas recipients: We do **not** routinely disclose personal information to overseas recipients, except as described below.

  *Personal information collected in New Zealand is securely transmitted to and processed in Australia using cloud-based infrastructure. We take reasonable steps to ensure that any overseas processing provides comparable safeguards to those required under New Zealand privacy law.*

  *We do not transfer personal information beyond Australia unless required for specific operational purposes, in which case appropriate safeguards will be applied.*

  *If this changes, we will update the policy, advise Clients and affected individuals (where reasonable).*

- 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 cloud-based infrastructure.
- Access to personal information (including image data) is strictly limited to authorised personnel and subject to logging and audit controls.
- Client staff access the App via role-based permission, 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 obligations under the Privacy Act 2020, including notifying the Office of the Privacy Commissioner (OPC) and affected individuals where a privacy breach is likely to cause serious harm.
- We maintain logs of who accessed, modified, or disclosed data, and conduct regular security risk assessments in accordance with applicable legal and regulatory requirements, including the Privacy Act 2020 and guidance issued by the Office of the Privacy Commissioner (OPC).

- We retain personal information only as long as necessary for the purpose for which it was collected (see section 5) 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 information to allow us to verify your identity and locate the relevant personal information.
- We will respond within a reasonable and practicable period, and no later than 20 working days, in accordance with the Privacy Act 2020. Where an extension is required, we will notify the individual within that period and provide a revised timeframe.
- Where we hold personal information on behalf of a Client, we may refer the request to the relevant Client or consult with them in order to respond appropriately.
- If we deny access or correction, we will provide reasons for denial (unless legally prohibited).
- If you believe that our information about you is incorrect (e.g., 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 Privacy Act 2020, the Information Privacy Principles, this Privacy Policy, or your privacy rights, you may lodge a complaint with us.
- We will acknowledge and respond to your complaint within a reasonable timeframe and will keep you informed of its progress and outcome.
- We will investigate complaints and take appropriate action where necessary to address any issues identified.
- If you are not satisfied with our response, you may refer your complaint to the Office of the Privacy Commissioner (OPC) at www.privacy.org.nz or by calling 0800 803 909.

## 2.8. OVERSEAS DISCLOSURE

As noted above, personal information collected in New Zealand is securely transmitted to, processed and stored in Australia using cloud-based infrastructure. We take reasonable steps to ensure that any overseas recipients provides comparable safeguards to those required under the New Zealand privacy laws.

We do not disclose personal information beyond Australia unless necessary for specific operational or legal purposes, and only where appropriate safeguards are in place in accordance with applicable laws.

## 2.9. CONTACT DETAILS

For any questions about this privacy policy, or to request access to or correction of your personal information, please contact:

**WatchGuard by COMS SYSTEMS LIMITED (www.watchguard.net.nz)**

Email: privacy@watchguard.net.nz

Phone: 0800 266 797

For privacy complaints, please contact:

Email: complaints@watchguard.net.nz

We encourage individuals to contact us first so we can attempt to resolve any concerns.

## 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 CUSTOM CLAUSES FOR BIOMETRIC/FACIAL RECOGNITION PROCESSING

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 technology to assist Clients in identifying individuals enrolled in the App for approved operational purposes, including VIP patrons or loyalty programme members (where applicable and consent given), and individuals subject to access restrictions such as trespassed, excluded or banned within the App.
- Facial recognition processing involves the generation and use of biometric templates derived from facial images to perform matching. This constitutes sensitive personal information under applicable privacy laws. We only carry out this processing where it is reasonably necessary for the purposes described in this Privacy Policy.
- Biometric processing may also include the analysis of facial images to generate limited attributes (such as estimated age ranges) where this supports the purposes described in this Privacy Policy.
- Client notice obligations: Clients are responsible for ensuring that appropriate and visible notice (such as signage) is provided at locations where the App is in use, including information about the use of facial recognition and how personal information is processed.
- Accuracy/human-oversight: System-generated matches and alerts are **subject to human review** by authorised staff before action is taken. Decisions are not made solely on automated processing.
- Data minimisation: We only collect and retain personal information, including images and associated identifiers, that is reasonably necessary for the operation of the App, including matching, verification, and audit purposes.

  Images are limited to cropped facial images (headshots) rather than full-frame imagery, to minimise the amount of personal information collected. These images may be securely stored for matching and operational purposes.

- Facial recognition processing is performed using secure, cloud-based processing services that analyse images to identify similarities. We do not independently store biometric templates generated through this process; instead, images are used to facilitate matching within the system.
- Retention/deletion: Information relating to matches, alerts, and associated records is retained in accordance with section 5 (Data Retention) and applicable laws, and is securely deleted or de-identified when no longer required.
- Risk-management: We maintain a Privacy Impact Assessment (PIA) for biometric processing and have identified and mitigated key risks, including misidentification (e.g., age estimation inaccuracies), bias, and unauthorised access, through appropriate technical and organisational safeguards (encryption, access logs, and independent audit).
- Biometric processing assessment: We have undertaken assessments of the proportionality of our biometric processing, including privacy risks and safeguards. A summary of this assessment is available on request (see section 2.9).
- Handling of vulnerable individuals: Where individuals may present a heightened safety or welfare concern, Clients are responsible for applying appropriate operational procedures in accordance with their policies and applicable laws.
- Training and audit: Authorised users of the App are required to undertake training on appropriate use and privacy obligations. We conduct periodic monitoring and audits of system usage for compliance and appropriate use.

### 3.2. INDIVIDUAL STATUS RECORD MANAGEMENT

- Clients are responsible for supplying, maintaining, and updating accurate records relating to individuals enrolled in the App, including VIP patrons or loyalty programme members (where applicable and consent given), individuals subject to access restrictions (such as trespass, exclusion or bans), and other Client-defined operational, safety and security designations, in accordance with applicable laws and any relevant regulatory or operational requirements.
- We process such records strictly for the purpose described in this Privacy Policy, including supporting match detection within the App. These records are securely transmitted and stored in encrypted form.

- When a match is identified, an alert is generated for authorised staff. Any action taken in response to an alert (such as restricting access or other operational responses) is the responsibility of the Client. This Privacy Policy governs the handling of personal information, and does not govern operational decision-making by Clients.
- We maintain audit logs relating to system use and match activity, including the date and time of events, location or system context, user access, match confidence levels, and any recorded follow-up actions. These logs may be made available to Clients for auditing, compliance, and operational review purposes.

### 3.3. SAFETY AND SECURITY-RELATED IDENTIFICATION

- The App may be used by Clients to identify individuals enrolled in the system for approved operational purposes, including individuals subject to access restrictions (such as trespass, exclusions or bans) and other Client-defined operational, safety or security designations.
- Where a match occurs, an alert is generated for authorised staff. Any response to an alert (such as denying access or taking appropriate safety measures) is determined and carried out by the Client in accordance with their policies and applicable laws.
- Clients are responsible for ensuring that appropriate notice is provided regarding the use of the system, including how personal information is collected and used in connection with safety and security processes.
- Where the App is used in connection with membership, loyalty or VIP programmes, Clients are responsible for ensuring that individuals are provided with clear information about the use of their personal information and, where required by applicable law, that appropriate consent or authorisation is obtained.
- The App is not intended to be used for generalised or indiscriminate biometric surveillance or profiling of individuals. Biometric processing is limited to the purposes described in this Privacy Policy, including identification, safety and security functions.
- Where the App is used to support additional features such as age estimation or similar analytics, such processing is carried out solely for safety, compliance, or operational purposes and in accordance with applicable laws.

- Any aggregated analytics (such as age or gender statistics) are generated using de-identified or anonymised data and do not identify individuals.

### 3.4. DISCLOSURE TO THIRD PARTIES

- Where we engage third-party service providers (such as cloud hosting providers, biometric processing services, and support contractors), those providers are subject to contractual obligations requiring them to protect personal information in accordance with applicable privacy, security, and confidentiality requirements.
- We do not disclose personal information to third parties except as described in this Privacy Policy or as required or authorised by law.
- Where personal information is disclosed to law enforcement agencies or regulatory authorities in connection with Client operations, such disclosure is generally initiated or authorised by the Client. We may assist with the secure transmission or information where required to do so under applicable laws or contractual obligations.

## 4. CLIENT RESPONSIBILITIES

As the Client using the App, you are responsible for:

- Ensuring that appropriate and visible notice is provided to individuals at locations where the App is in use, including informing individuals that facial recognition technology is being used and how their personal information is collected and used (e.g., “Facial recognition technology is in use at this location. Facial images are processed to identify individuals subject to exclusion or access restrictions.”).
- Supplying and keeping accurate records relating to individuals enrolled in the App, including VIP patrons or loyalty programme members (where applicable and consent given), individuals subject to access restrictions (such as trespass, exclusions or bans), and other Client-defined operational, safety or security designations, and updating those records promptly when circumstances change.
- Where the App is used in connection with membership, loyalty or VIP programmes, ensuring that appropriate information and consent (where required by applicable law) is obtained from individuals.

- Ensuring that authorised staff are properly trained in the use of the App, including match-response procedures, safety and security protocols, and appropriate handling of personal information.
- Ensuring that any actions taken in response to system alerts (such as restricting access or taking other safety measures) comply with the applicable laws, regulations, and internal policies.
- Providing individuals with access to this Privacy Policy (or a summary of it), and responding to enquiries regarding how personal information 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 match logs and image data associated with individuals linked to individual status records (such as membership, trespass, exclusion, or ban status) for the duration of that status and in accordance with applicable laws and regulatory requirements.
- We retain image data and associated logs that do not result in a match for up to 72 hours, during which time they may be accessed by authorised personnel for operational and security reasons.
- Following this period, such data may be moved to a restricted-access storage environment and retained for a further limited period (up to 30 days) for purposes such as incident investigation, system security, and responding to lawful requests (including from law enforcement or regulators). Access to this environment is strictly controlled.
- Where the system generates derived or analytical data (such as estimated age ranges or similar system-generated attributes), these are generally used in real time to support operational decision-making (e.g., prompting staff to verify identification) and not stored as part of an individual's record. Where such information is retained, it is either de-identified or aggregated so that it does not identify an individual.
- We do not store inferred attributes (such as estimated age or gender) as part of identifiable personal information records within the App.

- After the retention period expires, we securely delete or irreversibly de-identify the information (for example, by deleting image data and associated identifiers so that the information can no longer be used to identify an individual).
- We may retain aggregated, non-identifying statistical data (e.g., number of matches per month, system usage metrics or demographic trends) indefinitely for analytics, improvement, and compliance reporting, where that data does not identify individuals.

## 6. DATA BREACH AND INCIDENT RESPONSE

- In the event of an eligible data breach (unauthorised access, disclosure or loss of personal data), we will follow our incident response procedures and comply with our obligations under the Privacy Act 2020, including notifying the Office of the Privacy Commissioner (OPC) and affected individuals where the breach is likely to cause serious harm.
- We will also inform the Client without undue delay in accordance with applicable obligations, so that an appropriate and coordinated response can occur (including notification of affected individuals, regulatory reporting, and mitigation actions).
- 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 request access to personal information held about you, including confirmation of whether you are enrolled in the App, or are recorded as subject to trespass, exclusion, ban, or other safety and security-related status, and request correction where appropriate (subject to legal and regulatory requirements).
- You may choose not to engage with environments where the App is in use; however, you should note that access may be restricted to certain areas or circumstances, particularly where individuals are subject to access controls or restrictions applied by Clients.
- Individuals who voluntarily enrolled in a loyalty or VIP programme may withdraw their participation at any time. Upon receiving and verifying a request, the participating Client

must remove the individual's enrolment from the relevant loyalty or VIP watchlists unless it is required to retain information for a lawful purpose.

- You may ask questions or make a complaint if you believe your privacy has been breached (see section 2.7).
- You may request a copy of this Privacy Policy in an alternate format if required.

We will not discriminate or penalise individuals for exercising their rights.

## 8. GLOSSARY AND DEFINITIONS

- **APP:** The WatchGuard mobile/web application and associated services, operated under the "WatchGuard by COMS" brand and provided by COMS Systems Limited, in association with our client.
- **Banned status**: an individual formally prohibited from accessing a Client's location or services.
- **Biometric template**: a mathematical representation derived from facial imagery used for matching; it does not necessarily allow the reconstruction of the full image.
- **Client**: an organisation or business that uses the App within its operations and is responsible for supplying and managing relevant personal information.
- **Exclusion status**: an individual who is restricted from accessing a Client's location or services under Client policies or applicable laws.
- **Face-matching**: The process by which the captured face data is compared against the stored data to determine whether an individual corresponds to a person subject to trespass, exclusion, ban or other safety and security-related status.
- **Safety and security-related status**: an individual identified by a Client (or regulatory body) as requiring additional attention or restrictions for safety or security purposes in accordance with applicable laws and Client policies.

- **Trespass status:** an individual who is not permitted entry to a Client's location in accordance with Client policies or applicable laws.
- **VIP or Loyalty Status:** An individual enrolled by a Client for approved operational purposes, such as VIP recognition, loyalty programme participation, customer service, access management, or similar Client-defined purposes.
- **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 2.0, Ref: 3307601932, dated 13 July 2026. 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).