



WHITE PAPER

Facial Authentication and Biometrics: Privacy, Consent and Compliance by Design

A guide to biometric access control with privacy built in: modality and mode choices, consent, template handling, retention, vendor due diligence and audits.

By IoT Hybrid Solutions

BIOMETRICS

ACCESS CONTROL

PRIVACY

COMPLIANCE

FACIAL AUTHENTICATION



Executive summary

- Biometric access control can strengthen authentication and reduce credential sharing, but biometric data is sensitive and in many places specifically regulated. Design privacy in from the start.

- Choose the modality (fingerprint, face) and the verification mode (badge plus biometric, or biometric only) based on risk, throughput and privacy, not convenience alone.
- Consent, notice and a genuine alternative for people who decline are central to most programs. Work with counsel to define them for each jurisdiction.
- Minimize what is collected and where it is stored. Prefer templates over images, and consider storing templates on the credential where the risk model allows.
- Treat biometric vendors and systems as high-risk data processors: perform due diligence, define retention and deletion, and audit regularly.

This paper describes considerations and good practice. It is not legal advice. Laws governing biometric data vary by jurisdiction and change over time, so consult counsel before collecting biometric data.

Biometric options

Modalities

- **Fingerprint:** mature, compact and widely supported. Performance can vary with skin condition, gloves and dirty sensors. Requires contact, which some users and hygiene policies prefer to avoid.
- **Face:** contactless and fast at high throughput. Performance depends on lighting, camera position and enrollment quality. Facial authentication at a door, where a person presents to a reader, is distinct from facial recognition across camera networks, and the two should not be confused in design or communication.
- **Other modalities:** iris, palm vein and similar technologies suit specific high-security or hygiene-sensitive areas.

Verification modes

- **Badge plus biometric (one-to-one verification):** the person presents a credential, and the reader compares the live sample with the template linked to that credential. This confirms the credential holder is the person presenting it.
- **Biometric only (one-to-many identification):** the system compares the live sample against a database of enrolled templates to identify the person. This removes the badge but involves a central database and broader processing.
- **Biometric plus PIN or multi-factor:** used for the highest-risk spaces.

Choosing

- Use badge plus biometric where the goal is to stop credential sharing or to add a second factor to sensitive areas.
- Consider biometric only where throughput and convenience justify the additional data processing, and where legal review supports it.
- Match the mode to the door: data halls, labs, cash rooms and executive areas justify stronger controls than a general office entrance.

Consent and enrollment

Notice and consent

Many jurisdictions require some combination of written notice, stated purpose, retention schedule and consent before biometric data is collected. Requirements differ, and employee consent may be treated differently from visitor or contractor consent. Define, with counsel:

- What notice is given, in what form and when
- How consent is recorded and stored
- How a person can withdraw consent, and what happens to their data when they do
- Which alternative is offered to people who decline, such as badge plus PIN, with no penalty

Enrollment good practice

- Enroll in a controlled setting with trained staff, good lighting and a defined procedure
- Verify identity against an authoritative source before enrollment
- Capture the minimum samples needed for reliable matching
- Test the new template at a reader before the person leaves
- Record who enrolled whom, when and under which consent record
- Re-enroll on a defined schedule or when matching performance degrades

Enrollment checklist

- Written enrollment procedure and trained enrollers
- Notice provided and consent recorded before capture
- Alternative credential issued to anyone who declines
- Enrollment logged with consent reference

- No raw images retained unless there is a documented need

Data minimization and template handling

The less biometric data you hold, the less you have to protect.

Templates versus images

Most systems convert a fingerprint or face image into a template, a mathematical representation used for matching. Retaining only templates, and discarding enrollment images once the template is created, reduces exposure. Confirm with the vendor whether templates are proprietary, whether they can be reversed into images and how they are protected.

Where templates are stored

- **On the credential:** the template lives on the person's card or mobile credential, and the reader matches locally. No central biometric database exists. This suits badge plus biometric.
- **On the reader or controller:** templates are distributed to devices. Protect the devices physically and logically.
- **Central server:** templates are held in a database for distribution or one-to-many matching. This requires the strongest protection and the most careful legal review.

Security controls

- Encrypt templates at rest and in transit
- Use secure, supervised protocols between readers and controllers, such as OSDP with secure channel
- Segment biometric devices and servers on the network. Network configuration is typically the customer's IT team unless the integrator is contracted for it.
- Restrict administrative access by role, require strong authentication and log all access
- Keep reader firmware and server software current
- Separate biometric data from other personal data where the platform allows

Retention and deletion

Retention policy

Define in writing how long biometric data is kept and why. A common approach is to keep a template only while the person has an active need for access, and to delete it promptly when that need ends. Some jurisdictions set maximum retention periods, so confirm the rules with counsel.

Deletion triggers

- Employment or contract ends
- Access to the protected area is no longer needed
- Consent is withdrawn
- The retention period expires
- The system is decommissioned or replaced

Making deletion real

- Automate deletion from the identity lifecycle, so offboarding in HR or the identity provider removes the template
- Delete from every location: server, controllers, readers, backups and credentials where possible
- Obtain written confirmation from vendors and integrators that data has been deleted at the end of a pilot or contract
- Log deletions for audit

Regulatory landscape

Biometric data is regulated differently around the world, and the landscape is evolving. Stated generally:

- Some US states have laws specifically governing the collection, use, storage and destruction of biometric identifiers, and some of these include private rights of action. Others address biometrics through broader privacy laws.
- Other jurisdictions, including the European Union and the United Kingdom, treat biometric data used for identification as a special category of personal data with additional conditions for processing.
- Workplace rules, employee representation bodies and sector regulations may add requirements.
- Local laws may also address signage, notice and data transfers across borders.

Because these requirements vary and change, involve legal counsel and your privacy team before any biometric deployment, document the legal basis for each site, and review it when expanding to new jurisdictions. Where a data protection impact assessment is required or advisable, complete it before collection begins.

Vendor due diligence

Treat biometric vendors as high-risk processors. Ask:

- Where are templates created, stored and matched, and can we choose on-credential or on-device storage?
- Are enrollment images retained? Can they be disabled?
- How are templates encrypted, and who holds the keys?
- Can templates be reversed into images, or used outside your system?
- Does the vendor or any cloud service have access to biometric data? In which countries?
- What independent testing of matching accuracy and demographic performance has the vendor completed? Ask for documentation.
- What liveness or spoof detection is included?
- How does the system support consent records, alternative credentials and deletion?
- What security certifications, penetration testing and vulnerability disclosure practices does the vendor maintain?
- What happens to data at contract end?

Record the answers in your vendor risk process and revisit them at renewal.

Operations and audits

Day-to-day operations

- Monitor false reject rates by reader and adjust placement, lighting or enrollment where users struggle
- Keep an alternative credential path working at every biometric door
- Train security and front desk staff to explain the program and handle questions
- Route privacy questions and access requests to a named privacy contact

Audit program

- Reconcile enrolled templates against active, consented users at least quarterly
- Confirm deletions occurred for departed users
- Review administrative access logs to biometric systems
- Verify firmware and software currency
- Re-validate notices, consent forms and retention policy with counsel annually or when laws change

Roles

- **Program owner** (security leader): accountable for the biometric program
- **Privacy lead:** owns notices, consent, assessments and data subject requests
- **Legal counsel:** advises on jurisdictional requirements
- **IT security lead:** owns network segmentation, encryption and access controls
- **Access control administrator:** manages enrollment, templates and deletion
- **Integrator:** installs, configures and supports readers and integration

How IoT Hybrid Solutions can help

IoT Hybrid Solutions designs and installs biometric access control with privacy built in. We help select modalities and verification modes, configure template storage and secure reader protocols, integrate with your access control platform and identity lifecycle, and support audits through **managed services**. We work with biometric manufacturers such as Suprema and Alcatraz as examples and remain platform-agnostic. We coordinate with your counsel and privacy team rather than advising on law. See **access control** and **compliance**.

Next step

If you are planning facial authentication or fingerprint readers, start with the privacy design. **Contact us** to discuss your requirements.