FRACT Standard Governance Framework

for the Use of Live Facial Recognition in Self-Exclusion

Introduction

Why the FRACT Standard Exists

Self-excluders personal data is classified as health data and so, as special category data, already has a high compliance bar when being processed. The use of Live Facial Recognition (LFR) to support the detection of self-excluded individuals raises the compliance bar further and carries increased regulatory, operational, and reputational risk.

The **FRACT Standard (Facial Recognition Accreditation, Compliance & Technical Standard)** has been developed to provide a structured, defensible framework for assessing and governing the use of LFR technologies in self-exclusion environments.

It ensures that any deployed solution is:

- Lawful
- Proportionate
- Technically robust
- Operationally controlled
- Subject to ongoing oversight and governance

1. What the FRACT Standard Protects

The FRACT Standard protects:

- Self-excluded individuals
- Venue operators
- Technology providers
- The integrity of the self-exclusion schemes

It does this by ensuring that the core technology and the way it is used meet defined benchmarks for accuracy, security, compliance, and governance.

2. How FRACT Works – Three-Phase Accreditation Model

All LFR providers must complete a structured three-phase assessment:

Phase 1 – Initial Assessment

- Baseline review of suitability, transparency, governance maturity, and algorithmic credibility.

CONFIDENTIAL

© 2026 FacEProtect Ltd. Confidential. All rights reserved. Company Registration Number: 16817787

Phase 2 – Compliance & Technical Validation

- Detailed review of technical performance, security controls, data governance, and integration readiness.

Phase 3 – Legal, Operational & Governance Assurance

- Confirmation of lawful deployment, contractual clarity, operational readiness, and transparency controls.

Successful completion may result in FRACT Standard Certification, valid for a defined period and subject to annual review.

3. Technical & Compliance Benchmarks

The FRACT Standard establishes minimum expectations across:

- Technical accuracy and performance
- Bias and demographic performance considerations
- Security architecture and resilience
- Data protection compliance
- Lawful processing of biometric data
- Clear controller/processor role definition
- Data minimisation and retention controls
- Ongoing operational oversight and governance

Independent benchmarks, including recognised testing frameworks such as NIST FRVT, may be referenced as part of the assessment. However, accreditation is based on a holistic review rather than any single metric.

4. Ongoing Governance

FRACT certification is not a one-time approval.

Certified providers are subject to:

- Annual reassessment
- Review following material change
- Ongoing performance and compliance monitoring

Failure to maintain required standards may result in suspension or withdrawal of certification.

CONFIDENTIAL

© 2026 FacEProtect Ltd. Confidential. All rights reserved. Company Registration Number: 16817787

5. What This Means for Clients

For venue operators and scheme participants, the FRACT Standard provides:

- A structured and defensible governance model
- Reduced regulatory exposure
- Clear separation of roles and responsibilities
- Independent oversight of technology deployment
- Documented audit trail and reporting

6. Intellectual Property Notice

The FRACT Standard is the proprietary intellectual property of FacEProtect Ltd. All rights reserved.

CONFIDENTIAL

© 2026 FacEProtect Ltd. Confidential. All rights reserved. Company Registration Number: 16817787