AI GOVERNANCE HUB

Compliance Assessment Report

Document Information

Use Case:	Pilot deployment of live facial recognition (LFR) technology by Imm...
Document Type:	SYSTEM_SPEC
System Type:	Live Facial Recognition (LFR) system
Analysis Date:	11 December 2025
Frameworks Assessed:	UK ICO, UK DPA / GDPR

Executive Summary

57%	1	Moderate
UK ALIGNMENT	CRITICAL GAPS	COMPLIANCE

KEY RISKS:

- Contestability & redress mechanisms
- Transparency obligations (Art. 13/14)
- Absence of defined contestability and redress m...

Partial compliance with UK AI governance frameworks (UK Alignment Score: 57%). 1 critical gaps require remediation.

What This Means

This system has moderate compliance gaps that require attention before deployment. Without remediation, you may face regulatory scrutiny, enforcement action, or reputational risk.

Framework Scores

Priority Actions

1. Design and document end-to-end contestability and redress processes for individuals flagged by LFR, including clear notification (where appropriate), access to explanations, routes to challenge or correct decisions, and oversight of how challenges are handled.
2. Implement and record rigorous safety, security, and fairness controls for the LFR pilot, including pre-deployment and ongoing accuracy/bias testing, cybersecurity measures, clear retention limits for images and templates (especially for non-matches), and explicit proportionality and data minimisation safeguards aligned with ICO LFR guidance.
3. Define and document the role of human oversight, decision-making workflow, and data subject rights (including how individuals can obtain human intervention, express their view, and contest decisions) where LFR outputs are used operationally, to address Article 22 safeguards.
4. Design and implement a comprehensive transparency strategy for the Holyhead pilot (on-site notices, online privacy information, and routes to exercise rights) that clearly explains the controller, purposes, legal basis, use of LFR, retention, and complaint mechanisms.
5. Extend the DPIA (or associated documentation) to cover data minimisation, retention and deletion policies for non-matches and watchlists, and measures to test, monitor and mitigate bias and inaccuracies in the LFR system.

Framework Analysis

UK ICO AI Principles 55%

The DPIA shows strong governance and a clearly scoped pilot purpose, but current documentation falls short of ICO expectations on safety/robustness, fairness (including bias mitigation), contestability, and detailed data minimisation and privacy safeguards for live facial recognition in a high-risk law enforcement context.

Requirements:

Safety & Security	Partial
Fairness	Partial
Accountability & Governance	Met
Contestability & Redress	Not Met
Data Minimisation	Partial

Strengths

- Clear governance structure and accountability evidenced through a formal DPIA, identified IAO, project manager, data...
- Targeted pilot scope focusing on a specific law enforcement purpose (identifying individuals breaching Deportation Or...

Critical Gaps

- Absence of defined contestability and redress mechanisms for individuals affected by LFR matches, including

false pos...

- Lack of explicit safety, robustness, and bias-mitigation measures for the LFR system, including testing, monitoring,...

UK Data Protection Act / GDPR 60%

The project has a structured DPIA with senior sign-off and a clearly framed law-enforcement purpose, but current documentation does not yet demonstrate compliance with automated decision-making safeguards or transparency duties, and only partially evidences adherence to core data protection principles for live facial

Requirements:

Article 22 - Automated Decision...	No Evidence
Article 5 - Data Principles	Partial
Article 13/14 - Transparency	Not Met
Article 35 - DPIA	Met

Strengths

- A formal DPIA process has been initiated and taken through multiple draft versions to SRO and IAO sign-off, indicatin...
- The purpose of processing is narrowly described as identifying individuals re-entering in breach of Deportation Order...

Critical Gaps

- Absence of documented safeguards and rights information for any automated or semi-automated decisions arising from LF...
- Lack of a defined transparency approach for informing travellers and affected individuals about the LFR deployment an...

Detailed Findings

ICO

Safety & Security

No explicit evidence in the excerpt of technical robustness measures, safety testing, performance evaluation, or security controls for the LFR system (e.g. testing error rates, robustness against spoofing, or cybersecurity safeguards).

Fairness

Excerpt does not show assessment of demographic bias, equal error rates across protected groups, or explanation/transparency measures for affected individuals, particularly around proportionality and potential for discriminatory impacts.

Contestability & Redress

No evidence in the excerpt of mechanisms for individuals to challenge LFR matches, obtain explanations, exercise rights of access/objection, or routes for redress where false positives or wrongful interventions occur.

Data Minimisation

While scope is described as focusing on individuals on a deportation list at a single port, the excerpt does not specify limits on image retention, watchlist size, exclusion of non-watchlisted individuals, or technical minimisation measures (e.g. on-the-fly processing without storage of non-matches).

DPA

Article 22 - Automated Decision Making

DPIA excerpt does not indicate whether individuals are subject to solely automated decisions based on LFR matches, nor any safeguards (human review, contesting decisions, right to obtain human intervention).

Article 5 - Data Principles

Purpose is defined and limited to locating individuals breaching Deportation Orders, but there is no evidence on data minimisation (e.g. retention, non-match handling), fairness measures (bias testing, error handling) or proportionality assessments required for LFR.

Article 13/14 - Transparency

No information on how data subjects or the general public will be informed about the LFR pilot, controller identity, purposes, legal basis, data subject rights, or complaint routes at or before the point of data capture.