AI GOVERNANCE HUB

Compliance Assessment Report

Document Information

Use Case:	Live Facial Recognition (LFR) deployment by South Wales Police for...
Document Type:	SYSTEM_SPEC
System Type:	Live Facial Recognition (LFR) biometric identification system
Analysis Date:	11 December 2025
Frameworks Assessed:	UK ICO, UK DPA / GDPR, EU AI Act, ISO/IEC 42001

Executive Summary

61%
UK ALIGNMENT

1
CRITICAL GAPS

Moderate
COMPLIANCE

KEY RISKS:

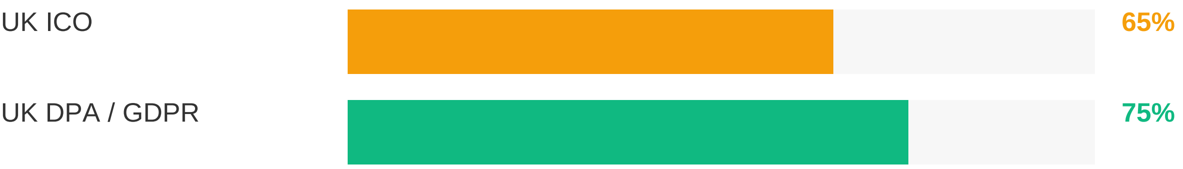
- Contestability & redress mechanisms
- Transparency obligations (Art. 13/14)
- Complete absence of contestability and redress...

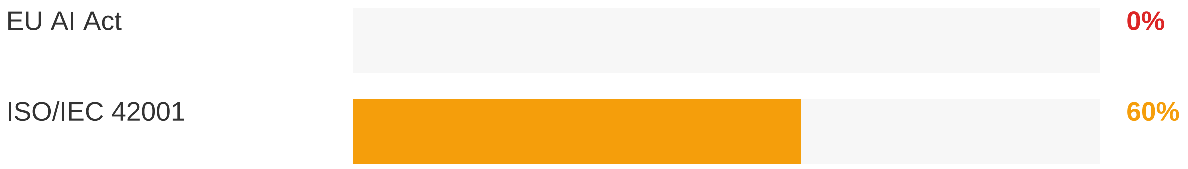
Partial compliance with UK AI governance frameworks (UK Alignment Score: 61%). 1 critical gaps require remediation.

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. Implement and document clear contestability mechanisms allowing individuals to challenge LFR matches and seek redress
2. Develop and implement comprehensive fairness testing protocols across demographic groups with documented results
3. Implement mandatory public signage and advance notification protocols for all LFR deployments
4. Conduct and document demographic bias testing with mitigation strategies
5. Implement comprehensive data quality controls and lifecycle management

Framework Analysis

UK ICO AI Principles 65%

The DPIA demonstrates strong accountability structures and adherence to data minimization principles with human oversight of system outputs. However, it lacks critical contestability mechanisms and comprehensive fairness testing procedures, representing significant compliance gaps that require immediate attention to meet

Requirements:

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

Strengths

- Clear accountability structure with named responsible owners and authorization hierarchy
- Strong emphasis on 'strictly necessary' standard for data processing under DPA 2018

Critical Gaps

- Complete absence of contestability and redress mechanisms for individuals
- Lack of documented fairness testing procedures across demographic groups

UK Data Protection Act / GDPR 75%

The LFR system demonstrates strong compliance with DPIA requirements and includes necessary human oversight. However, critical gaps in public transparency and demographic fairness assessments prevent full GDPR/DPA compliance, particularly given the Court of Appeal's previous ruling on South Wales Police's AFR

Requirements:

Article 22 - Automated Decision...	Met
Article 5 - Data Principles	Partial
Article 13/14 - Transparency	Not Met
Article 35 - DPIA	Met

Strengths

- Clear human oversight process preventing solely automated decisions
- Comprehensive DPIA addressing necessity and proportionality requirements

Critical Gaps

- Absence of public transparency measures for LFR deployments
- Insufficient fairness safeguards regarding demographic bias

ISO/IEC 42001:2023 60%

The document demonstrates partial compliance with ISO/IEC 42001:2023 requirements. It has strong elements in monitoring (human oversight) and basic governance framework, but lacks comprehensive data quality and lifecycle management, and has limited risk management controls beyond basic DPIA and human oversight. The

Requirements:

Governance Framework	Partial
Risk Management	Partial
Data Quality & Lifecycle	Not Met
Monitoring & Incident Response	Met

Strengths

- Clear human oversight process
- Defined scope and purpose

Critical Gaps

- Lack of comprehensive data quality and lifecycle management
- Limited risk treatment plan with specific controls

Detailed Findings

ICO

Safety & Security

No specific details about security measures, robustness testing across different conditions (lighting, angles, demographics), or failure mode handling procedures

Fairness

No specific details about testing for bias across demographic groups, fairness monitoring procedures, or transparency measures for individuals being processed

Contestability & Redress

No details about how individuals can contest matches or decisions, redress mechanisms for incorrect identifications, or complaint procedures related to the LFR system

DPA

Article 5 - Data Principles

Limited discussion of fairness considerations regarding demographic bias; no evidence of bias testing across gender/ethnic groups despite Court of Appeal ruling highlighting this risk

Article 13/14 - Transparency

No evidence of public transparency measures such as signage, advance notification, or accessible information about LFR deployments in public spaces as required by GDPR

ISO 42001

Governance Framework

Limited information on top management commitment to AI governance; No explicit AI governance policy document

Risk Management

Limited discussion of bias risks in facial recognition; No specific metrics for measuring risk; Limited discussion of ethical risks beyond data protection; No clear risk treatment plan with specific controls beyond human oversight

Data Quality & Lifecycle

No specific data quality metrics or controls; No validation procedures for data quality; Limited information on data retention periods; No clear process for data lifecycle management beyond basic operational stages