South Wales Police and Gwent Police

Data protection audit report

August 2025

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and other data protection legislation. Section 146 of the DPA 2018 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA 2018 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

South Wales Police (SWP) and Gwent Police (collectively abbreviated as SWGP) agreed to a consensual audit of its data protection practices.

As part of the ICO's AI and biometrics strategy, the ICO has committed to supporting and ensuring the proportionate and rights-respecting use of facial recognition technology (FRT) by the police by auditing police forces using FRT and publishing the findings, securing assurance that deployments are well-governed and people's rights are protected.

The purpose of the audit is to provide the Information Commissioner and SWGP with an independent assurance of the extent to which SWGP within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of SWGP's processing of personal data. The scope may take into account any data protection issues or risks which are specific to SWGP, identified from ICO intelligence or SWGP's own concerns, or any data protection issues or risks which affect its specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of SWGP, the nature and extent of SWGP's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to SWGP.

It was agreed that the audit would focus on the following area(s):

Scope area	Description
Live Facial Recognition Technology	Where an organisation uses live facial recognition (LFR) technology, the extent to which the use is necessary and proportionate, its design meets expectations of fairness and accuracy, and the end to end process is demonstrably compliant with data protection legislation.
Retrospective Facial Recognition Technology	Where an organisation uses retrospective facial recognition (RFR) technology, the extent to which the use is necessary and proportionate, its design meets expectations of fairness and accuracy, and the end to end process is demonstrably compliant with data protection legislation.

During the audit, the SWGP pilot scheme of Operator Initiated Facial Recognition Technology (OIFR) was also observed. Given the pilot is in its infancy, rather than make formal recommendations for SWGP to accept or reject upon the conclusion of this audit, the ICO has provided feedback based on what was observed for SWGP to incorporate into their learnings as the pilot scheme progresses.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, both on-site and remote interviews with selected staff, an inspection of selected records, demonstrations of facial recognition technology and a virtual review of evidential documentation.

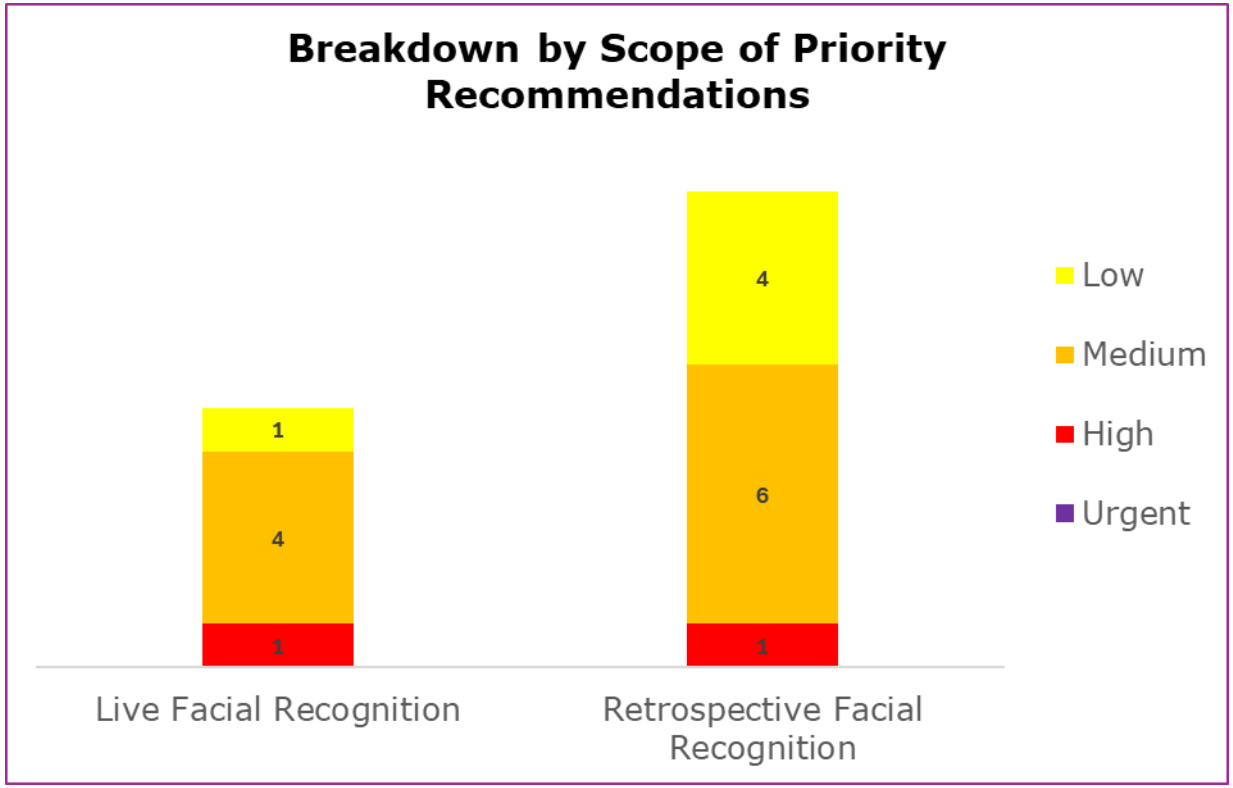
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist SWGP in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. SWGP's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Live Facial Recognition Technology	High	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.
Retrospective Facial Recognition Technology	High	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.

The assurance ratings above are reflective of the hybrid audit methodology deployed and the rating may not necessarily represent a comprehensive assessment of compliance.

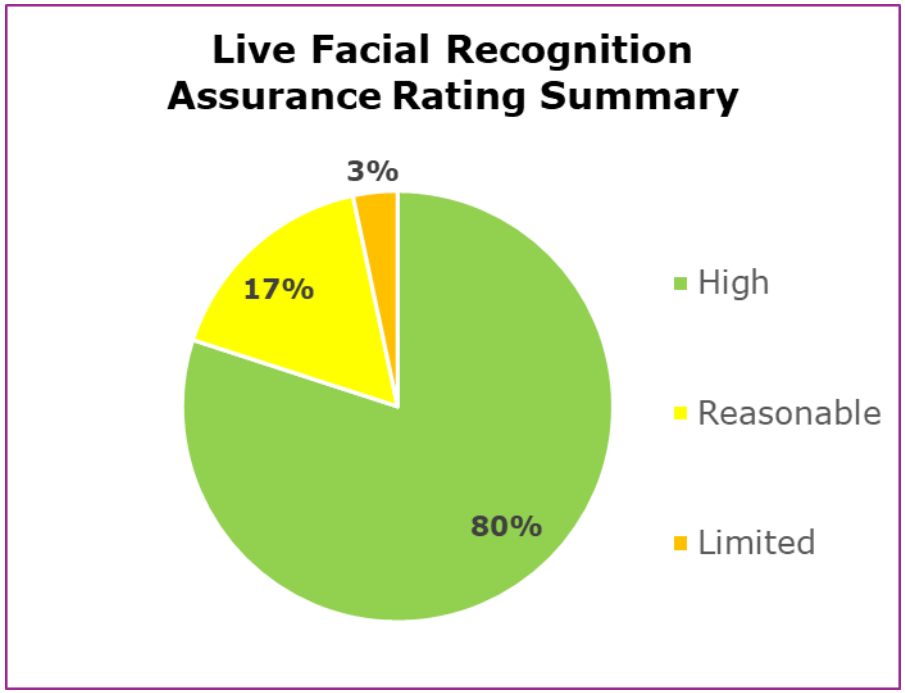
Priority Recommendations



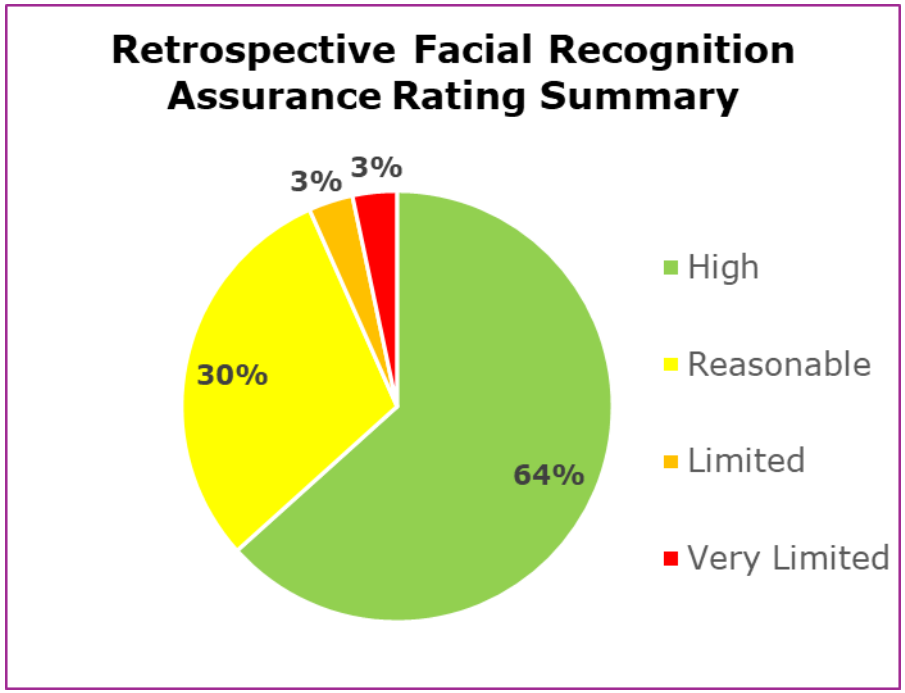
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- LFR scope area has one high, four medium and one low priority recommendations
- RFR scope area has one high, six medium and four low priority recommendations

Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the LFR scope. 80% high assurance, 17% reasonable assurance, 3% limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the RFR scope. 64% high assurance, 30% reasonable assurance, 3% limited assurance, 3% very limited assurance.

Key areas for improvement

We identified some key areas within our audit where SWGP needed to implement further measures to comply with data protection law.

Live Facial Recognition (LFR) Technology (applies to SWP only)

- Ensure that retention periods are accurately and consistently documented across all core records.
- Policies and procedures should be reviewed at appropriate intervals to maintain their accuracy and relevance. Full version control information should be shown, and staff should be notified of any changes.

Retrospective Facial Recognition (RFR) Technology

- Review RFR documentation to ensure that information on retention of RFR data is located where indicated.
- Document version control should consistently reflect changes made during reviews.
- Ensure that documents relating to RFR are reviewed at appropriate intervals.

Key areas of assurance

At the time of the audit and based on the evidence seen by auditors, measures were in place and implemented effectively to meet the control objectives in the following key areas.

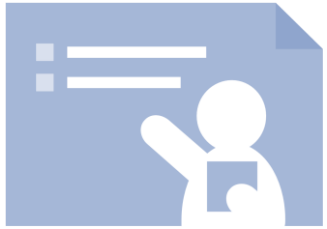
Live Facial Recognition (LFR) Technology

- A privacy management framework is embedded and endorsed by senior management. It supports the use of LFR, and data flows for the use of LFR are comprehensively mapped.
- SWP can demonstrate the lawful provenance of the images used to generate biometric templates for LFR watchlists.
- A data protection impact assessment (DPIA) procedure is in place. DPIAs are completed following consultation with all appropriate internal and external stakeholders, and the DPO has oversight responsibility.
- Data collected for LFR is adequate, relevant and limited to what is necessary for its purpose.
- Individuals are informed about the use of LFR technology in a clear and accessible manner, and SWP actively engages with the public during LFR deployments.

Retrospective Facial Recognition (RFR) Technology

- The record of processing activities (RoPA) entries for RFR are clear and give a good understanding of the processing activity undertaken as part of RFR.
- Every use of RFR is assessed afterwards, and statistics are reported at appropriate oversight meetings.

Appendices



Appendix One – Recommendation Priority Ratings Descriptions

Urgent Priority Recommendations These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation.
High Priority Recommendations These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.
Medium Priority Recommendations These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.
Low Priority Recommendations These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of South Wales Police and Gwent Police.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of South Wales Police and Gwent Police. The scope areas and controls covered by the audit have been tailored to South Wales Police and Gwent Police and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.