SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Agenda Item 4.2

Meeting	**SPA Audit, Risk and Assurance Committee**
Date	**6 February 2024**
Location	**Video Conference**
Title of Paper	**ICO Audit - Mobile Phone Data Extraction Project – Review Report**
Presented By	**Deputy Chief Constable Professionalism**
Recommendation to Members	**For Discussion**
Appendix Attached	**Yes:** **Appendix A – ICO Report** **Appendix B – Dashboard & Action Tracker**

PURPOSE

To provide the Audit, Risk and Assurance Committee with an initial update following a review of Police Scotland's mobile phone data extraction processing activities.

Members are invited to discuss the report.

1 BACKGROUND

1.1 In June 2020, the ICO published reports into the practice of mobile phone data extraction by police forces in the United Kingdom.

1.2 In May 2022, the Information Commissioner published an Opinion titled "Who's Under Investigation? The processing of victim's personal data in rape and serious sexual offence investigations," building upon the foundations established through the initial investigation into mobile phone extraction and introducing additional recommendations for police forces when acquiring data from victims' electronic devices and third party organisations.

1.3 The ICO committed to monitoring progress made by police forces towards ensuring that the data protection issues identified were appropriately addressed.

1.4 In line with that commitment and with the support of the National Police Chiefs Council, ICO commenced a project to assess the extent to which police forces have implemented the recommendations from their reports and embedded them into operational practice.

1.5 The terms of reference for the project stated that the organisations involved in the project would be kept confidential and therefore have not been published.

1.6 The review follows up on the recommendations from the 2020 reports, which have been completed or, are superseded by continuous improvement recommendations and highlight any areas of risk to their compliance.

1.7 The review also assessed the extent to which PSoS demonstrates best practice in their data protection governance and management of mobile phone data extraction.

1.8 Recommendations have been assessed as per Police Scotland's Internal Audits risk grading structure as Moderate.

	Moderate risk exposure - controls are not working effectively and efficiently and may create moderate risk within the organisanisation

2 FURTHER DETAIL ON THE REPORT

2.1 Refer to Appendix A – ICO Report

2.2 Refer to Appendix B – Dashboard and Action Tracker

3 FINANCIAL IMPLICATIONS

3.1 There are no "direct" financial implications associated with the Report.

4. PERSONNEL IMPLICATIONS

4.1 There are no personnel implications in this report.

5. LEGAL IMPLICATIONS

5.1 It is likely there are legal implications in this report given that any non-compliance of Data Protection legislation may be subject of civil claim for material/non-material harm.

6. REPUTATIONAL IMPLICATIONS

6.1 There are no reputational implications in this report.

7. SOCIAL IMPLICATIONS

7.1 There are no social implications in this report.

8. COMMUNITY IMPACT

8.1 There are no community implications in this report.

9. EQUALITIES IMPLICATIONS

9.1 There are no equality implications in this report.

10. ENVIRONMENT IMPLICATIONS

10.1 There are no environmental implications in this report.

All recommendations will have implications which will be assessed in detail during implementation.

RECOMMENDATIONS

Members are invited to discuss the report.

Police Service of Scotland

Mobile Phone Data Extraction (MPE) Project Review Report

October 2023

Executive summary

Background

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UKGDPR), the Data Protection Act 2018 (DPA18) and other data protection (DP) legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

In June 2020, the ICO published reports into the practice of mobile phone data extraction (MPE) by police forces in England and Wales. Further reports covering Northern Ireland and Scotland were published in June 2021. The reports presented the findings from the investigation, as well as making recommendations to improve the consistency of police forces' approach to MPE.

ICO investigation into mobile phone data extraction by police in the UK, the reports presented the findings and recommendations of an investigation carried out by the ICO.

Additionally, In May 2022 the Information Commissioner published an Opinion titled "**Who's Under Investigation? The processing of victim's personal data in rape and serious sexual offence investigations**," building upon the foundations established through the initial investigation into mobile phone extraction, and introducing additional recommendations for police forces when acquiring data from victims' electronic devices and third party organisations.

The Commissioner recognises the absolute right to a fair trial and the important part that relevant mobile phone data, and requests for data held by third party organisations, might play in criminal investigations and fair proceedings, and that this processing has the potential to bring about marked improvements to their quality and outcome. However, the use of these complex data extraction tools comes with inherent risks to the processing of personal data and thus compliance with DP legislation.

In the conclusions to these reports the Information Commissioner committed to monitoring progress made by police forces towards ensuring that the data protection issues identified were appropriately addressed. In line with that commitment and with the support of the National Police Chiefs Council (NPCC), we commenced a project to assess the extent to which police forces have implemented the recommendations from our reports and embedded them into operational practice. In addition, we're taking the opportunity to update our knowledge of how this activity is being undertaken within the sector.

The Police Service of Scotland (PSoS) has agreed to a review of their mobile phone data extraction processes and procedures by the ICO.

Scope

As with police forces in England, Wales and Northern Ireland, the ICO requested the completion of two questionnaires sent to the Data Protection Officer (DPO) and Operational Lead within Police Scotland. The next stage involved us undertaking more in-depth work on-site, to gain a clearer understanding of how mobile phone data extraction is undertaken in practice.

The primary purpose of the review is to follow up on the recommendations from the bespoke ICO investigation report for Police Scotland. This will provide the ICO and PSoS with an independent opinion of the extent to which PSoS are complying with data protection legislation when extracting personal data from mobile devices, and highlight any areas of risk to their compliance. The review will also assess the extent to which PSoS demonstrates best practice in their data protection governance and management of mobile phone data extraction.

Reviews 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 forms and a virtual review of evidential documentation.

Originally, the auditing toolkit used for this project was created based on Part 3 DPA 2018 legislative requirements and the 13 recommendations and risks within the original investigation report for police forces in England and Wales. The toolkit has been further developed to include the recommendations within the bespoke ICO investigation report for PSoS (see appendix one) and the recommendations from the Information Commissioner's Opinion on the processing of victims' personal data in rape and serious sexual offences (RASSO) investigations (appendix two).

Reporting

This report contains findings, recommendations, and best practice where appropriate. The intent of the report is to focus PSoS' attention on those control areas requiring action to mitigate information risks and improve compliance.

The ICO will use the responses and/or findings from this project to identify and analyse common themes and patterns which would then be used to produce an outcomes report and, potentially, to feed into new or updated guidance. These documents will be published on the ICO website and shared with the sector; however, individual police forces will not be identified in any outcomes/update report.

Survey responses

The two questionnaires sent to the DPO, and Operational Lead, were completed with supporting documentation submitted, as requested, for review. The last section of each survey covered third party requests, which both the DPO and Operational Lead were unable to answer as they stated the questions were not applicable to digital forensics.

Domains

This review focussed on the following area(s):

A. Governance
B. Information Risk
C. Appropriate Policy Document (APD)
D. Training and Awareness
E. Data Protection Compliance and Assurance
F. Lawful Basis
G. Transparency
H. Limited Purpose
I. Data Minimisation
J. Accuracy
K. Storage Limitation
L. Security
M. Data Protection by Design and Default
N. Data Protection Impact Assessments (DPIA)
O. Record of Processing Activities (RoPA)
P. Rape and Serious Sexual Offence (RASSO)

Overview of System and Data Processing

PS operate a two-tier system for MPE. They use cyber kiosks, which are purpose-built, standalone devices that allow officers and staff to view data stored on a range of digital devices, and have Digital Forensic Hubs (DFUs) across the North, West and East of Scotland which provide the core MPE capability, including extraction levels 1 (configured logical extraction), 2 (logical and physical extraction) and 3 (specialist extraction and examination).

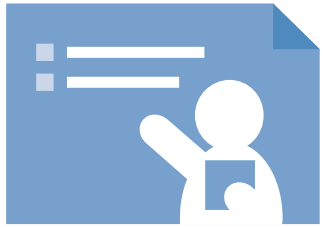
There are currently 41 cyber kiosks in use across PSoS, which are used by trained kiosk operators. Within the DFUs there are forensic analysists, team leaders and coordinators who are responsible for conducting and overseeing extractions.

When making a request for device examination, investigating officers are required to complete an Examination Request Form (ERF) and a relevant Digital Processing Notice (DPN). These documents are firstly submitted to a supervisor for an initial review, and then forwarded to the Cybercrime Gateway to either be approved for examination or rejected.

Dependant on the case, requests can be submitted for examination either via a cyber kiosk, where a kiosk operator will triage the device and establish whether there is anything of likely evidential value. If there is relevant material, then the officer is required to submit a revised ERF, via the supervisor, with specifics of the DFU examination required. Requests can also be submitted straight to a DFU.

As PSoS are conducting MPE for law enforcement purposes (most commonly the investigation of criminal offences), the personal data extracted from mobile devices is likely to be highly sensitive. As explained within the ICO investigation report, police practitioners cannot be certain about the nature of the data before viewing it and therefore should proceed on the assumption that it is sensitive and is being processed under Part 3 of the DPA18.

Review Findings



The areas for improvement that were identified in the course of our review are detailed below including recommendations in relation to how those improvements might be achieved. Where observations have been made these include suggestions to assist PSoS with possible enhancements to current practice.

Areas for Improvement

- Ensure appropriate written agreements are in place with the Crown Office Procurator Fiscal Service (COPFS) for any processing activities where both parties are acting as joint data controllers.
- Review all policies and/or procedures relating to MPE which are accessible to staff, to ensure the content is up to date and follows the correct process, including the requirement to complete a DPN and provide a copy to victims and/or witnesses.
- Ensure any training on the use of MPE for investigating officers adequately covers the relevant DP requirements.
- Ensure the end to end process for MPE is captured within the Information Asset Register (IAR)/Record of Processing Activity (RoPA) to ensure the processing of personal data through the use of MPE is formally documented and risk assessed.

Detailed Findings

Scope area: A. Governance and Accountability

Findings:

A1 – Cyber Investigations and Digital Forensics (CIDF) provide the MPE forensic capability for PSoS. Responsibility and accountability for information governance (IG) and DP matters surrounding MPE are assigned to several staff members across PSoS, including the DPO, the Senior Information Risk Owner (SIRO), Information Manager and senior staff members within CIDF, including a Detective Chief Inspector, who is the Operational Lead and a Detective Superintendent, who is the Tactical Information Asset Owner.

A2 - During interviews, ICO Auditors were informed that PSoS are engaging with the work the UK Government, the NPCC and the College of Policing are undertaking with respect to MPE (as per recommendation 6 within the ICO investigation report). As mentioned previously, investigating officers are required to complete and attach a relevant DPN form when submitting an ERF. On the PSoS external website, their Digital Device Examination by Agreement page refers to the Police, Crime, Sentencing and Court (PCSC) Act, specifically s.39(3) which requires a victim and/or witness to receive information regarding the acquisition and extraction of their device. During interviews PSoS also mentioned that they are adhering to the Home Office Extraction of Information from Electronic Devices: Code of Practice.

A3 – For some processing activities, PSoS and COPFS are joint data controllers. There are legal obligations within Part 6 of the Criminal Justice and Licensing (Scotland) Act 2010 which require PSoS to provide COPFS with all relevant information obtained or generated during the course of an investigation. This would include information that had been obtained through the use of MPE. During interviews, ICO Auditors were informed that COPFS may instruct PSoS to conduct further extractions if required for prosecution purposes. Additionally, section 15.3 of the Evidence in Criminal Proceedings 2010 Statutory Code of Practice, as referenced within COPFS sensitive records policy, states that COPFS may instruct PSoS to carry out particular lines of enquiry which may include the recovery of records from third parties. There is currently no documented arrangement between PSoS and COPFS that sets

out agreed roles and responsibilities for compliance with DP through the course of these joint controller relationships.

A4 – During interviews, ICO Auditors were informed that the DPO has sufficient oversight on the use of MPE and is consulted on its use as appropriate. The DPO meets on a monthly basis with senior staff members within CIDF to discuss statistical performance and is said to have oversight of the cyber kiosk DPIA and overarching DPIA for all data processing within CIDF, however no DPO advice has been recorded on the copies of the DPIAs provided.

A5 – PSoS have a Data Governance Board where DP/IG matters are discussed. The DPO and Senior Asset Owner for CIDF sit on this board, and during interviews ICO Auditors were informed that relevant risks relating to MPE would be reported to this board.

A6 – PSoS provided a significant number of documents relating to the use of the cyber kiosks and MPE. During interviews, ICO Auditors were shown the intranet where relevant policies and/or procedures are kept, which included guidance for submitting ERFs, the digital device examination principles and the cyber kiosk toolkit. The suite of documents provided by PSoS also included a number of process workflows. However, during interviews ICO Auditors were informed that some of these workflows are no longer in use.

Recommendation:

A3 – S.58 of the DPA18 states that where two or more competent authorities jointly determine the purposes and means of processing personal data, they are joint controllers. S.58(2) states that joint controllers must, in a transparent manner, determine their respective responsibilities by means of an arrangement. PSoS and COPFS must have appropriate agreements are in place for any processing activities where they are acting as joint data controllers, which must clearly and transparently set out each of their responsibilities under Part 3 of the DPA18. There is more guidance on joint controller relationships on the ICO website.

Accepted: Yes

Management Response: A joint controller agreement between PSoS and COPFS will be created that sets out clearly the processing activities and roles and responsibilities as provisioned by Part 3 of the DPA 18.

At this time Police Scotland has many ICO recommendations to implement following 3 separate audit strands which occurred simultaneously. These are being prioritised and those recommendations which are related to sensitive processing are being expedited. However, it is prudent to recognise that the interdependency with partner organisations can impact on timescales therefore realistic and achievable implementation dates must be set.

Action owner: SIRO

Implementation date: 1 May 2024

A4 – In order to demonstrate compliance with the accountability principle, PSoS should ensure any advice provided by the DPO is recorded on the DPIA, so that they are able to evidence that DPO advice has been provided and considered.

Accepted: Yes

Management Response: A review of org. structure, roles & responsibilities is being undertaken to ensure that the DPO can carry out their role effectively and specific to their ability to monitor compliance with legislation, policies, awareness raising and audits.

As part of this, the DPIA process will be amended to include a section for DPO advice & recommendations to be documented prior to approval being sought from SIAO.

The DPO has commented separately on the DPIA and evidence of this is attached at APPENDIX PSOS01

Action owner: SIRO

Implementation date: 1 April 2024

A6 – PSoS should review all policies, procedures and guidance documents that were submitted to the ICO and assess which documents remain applicable to the use of the cyber kiosks and MPE. Any outdated documents should be removed from circulation, to ensure staff are following the correct process.

Accepted: Yes

Management Response: A review of the suite of documentation which supports the process and procedures associated with the use of cyber kiosk and MPE is being undertaken in respect of this recommendation and also in support of preparation for ISO 1705 accreditation to ensure that only current, accurate information is available for staff access, mitigating any risk of non-compliance with current procedure.

Action owner: SIRO

Implementation date: 1 April 2024

Scope area: B. Information Risk

Findings:

B1 – During interviews ICO Auditors were informed that there is a risk register for CIDF, where risks relating to MPE are recorded if identified. Significant information risks should be reported to the DPO and/or SIRO if they meet the criteria. Risks from CIDF were submitted as evidence; while these examples are not specific to MPE they do evidence how risks are recorded within PSoS. Each risk is RAG rated, has a description of the risk, a nominated risk owner and review date.

Scope area: C. Appropriate Policy Document

Findings:

C1 - In response to question 22 of the DPO MPE project questionnaire:

"Does PS have an Appropriate Policy Document (APD) in place which covers MPE practice?"

The DPO answered *"yes".*

PSoS have an APD in place which details their justification for sensitive processing as required by s.35 and 42 of the DPA18, which is accessible via their website. During interviews, ICO Auditors were informed that PSoS do not rely on consent as a lawful basis and/or condition for sensitive processing, however their APD makes reference to the use of consent including the requirements of consent, i.e. being able to withdraw your consent at any time.

Recommendation:

C1 - Due to the complexity of the data extraction tool and the sensitivity of the personal data being processed, PSoS may wish to create a separate APD for MPE processing, to ensure they have fully considered and documented their justification for the activity and sensitive processing, as required by s.35 and 42 of the DPA18. Any separate APDs should document the lawful basis and/or condition for sensitive processing being relied upon for that processing activity.

Accepted: Yes

Management Response: A separate APD will be created for MPE.

Action owner: SIRO

Implementation date: 1 January 2024

Scope area: D. Training and Awareness

Findings:

D1 - In response to question 9 for both the DPO and Operational Lead surveys:

"*Does PS provide applicable staff with tailored and specific training on the use of MPE?"*

Both the DPO and Operational Lead answered "*yes*".

During interviews, ICO Auditors were informed that both the kiosk operators and forensic analysts receive training on the use of the cyber kiosks and the extraction software, however it was unclear what DP requirements the training covered. Additionally, investigating officers do not receive any official training on the use of MPE. The CIDF intranet page includes links to a number of useful documents relating to MPE, including the ERF, the digital device examination principles and the cyber kiosk toolkit, and during interviews ICO Auditors were informed that there are some 'how to' videos for staff to use, but the content of these videos were not provided as evidence and it was unclear whether they are mandatory.

Recommendation:

D1 – PSoS should ensure there is appropriate training on the use of MPE for investigating officers which adequately covers DP requirements. If PS decide that a series of 'how to' videos on the CIDF intranet page is sufficient, as a minimum these videos should cover:

- the lawful basis for processing (including sensitive processing);
- privacy information;
- the DP principles;
- the completion of the relevant DPN form;
- the use of MPE should be strictly necessary, proportionate, justified and relevant to a reasonable line of enquiry.

The use of these videos should be mandatory and form part of any overarching training programme for investigating officers and authorising supervisors. It should be reflected within a training needs analysis to ensure training requirements are formally documented.

Accepted: Yes

Management Response: The Cyber and Digital Forensics Learning and Development Co-ordinator has the lead on developing a training pathway to be used 'in-house' by Police Scotland for future Cyber Kiosk Operators. This

is founded heavily on the vendors original training package, but the training will be designed to ensure it adequately covers DP requirements.

It is not the case at this stage that the training package will include 'how to' videos.

The 'how to' videos were created to refresh knowledge since the initial training and are seen as a step by step guide to conducting some of the most common operator tasks.

Action owner: SIRO

Implementation date: 1 May 2024

Scope area: E. DP Compliance and Assurance

Findings:

E1 – PSoS have been monitoring their progress with the completion of the recommendations from both the ICO investigation report on MPE and Information Commissioner's Opinion on RASSO. During interviews, the SIRO mentioned that the Force Audit and Risk Board has overall responsibility for monitoring progress with the recommendations and that they are a standing agenda item. On request, PSoS have been providing updates to the ICO's Scotland Office by responding to queries listed against each recommendation.

E2 - During interviews, ICO Auditors were informed that there is currently insufficient resource to introduce a programme of risk based internal DP and IG audits within PSoS. Without an extensive audit programme which covers high risk processing activities such as MPE, PSoS can have no assurance that their risk management is sufficient or effective. Risk of non-conformance with sections 70 and 71 of the DPA18.

Recommendation:

E2 - PSoS should introduce a programme of internal audits and/or compliance checks and should ensure the programme covers high risk processing activities such as MPE, to gain assurance that applicable staff are following

the correct procedures. PSoS should ensure any audit and/or compliance checks adequately cover IG/DP requirements.

Accepted: Yes

Management Response: Consideration will be given as to how best this recommendation might be delivered in a resource efficient manner across all PSoS high-risk processing activities.

In addition, the external audit roadmap for 2024/25 is being reviewed to ascertain whether feasible to include MPE specifically.

Action owner: SIRO

Implementation date: 1 May 2024

Scope area: F. Lawful Basis

Findings:

F1 – In response to question 17 and 18 of the DPO survey:

"What lawful basis does Police Scotland rely on to process personal data which is extracted from mobile devices?" and *"What condition for processing does Police Scotland rely on to process sensitive personal data extracted from a mobile device?"*

PSoS answered *"Necessary for the performance of a task carried out for a law enforcement purpose by a competent authority"* and *"Strictly necessary for the law enforcement purpose and meeting a condition in Schedule 8 DPA 2018".*

However, they also answered "*Yes*" in response to question 19 of the DPO survey:

"When relying on consent to process personal and sensitive data extracted from a mobile device, does Police Scotland keep a record of what the victim, witness or suspect has consented to?".

PSoS have actively steered away from the use of the term 'consent' when conducting MPE, to try and mitigate any confusion about whether consent is used as a lawful basis and/or condition for processing personal data that is extracted from mobile devices. PSoS now ask for 'agreement' to acquire a mobile device conduct MPE, however they are not relying on consent as a lawful basis and/or condition for processing. During interviews, some staff referred to the use of consent when conducting MPE, which may suggest that this change in 'consent' to 'agreement' may not be fully embedded.

Recommendation:

F1 – PSoS should continue to actively promote the use of 'agreement' instead of 'consent' when acquiring a mobile device from a victim and/or a witness for the use of MPE. Procedural documentation on MPE that is currently available for access should be reviewed to ensure consistency in the chosen terminology. This will help to ensure that when investigating officers are asking for agreement to acquire a mobile device, the communication is clear and data subjects are not being misinformed on the use of consent for the processing of their personal data.

Accepted: Yes

Management Response: (a) A review of procedural documentation is underway to ensure consistency and accuracy of lawful basis being cited.

(b) Tactical guidance regards the active promotion of the use of 'agreement' as opposed consent will be created and promoted throughout PSoS - consideration is being given to this being a multi-layered approach.

Action owner: SIRO

Implementation date: (a) 1 January 2024 (b) 1 May 2024

Scope area: G. Transparency

Findings:

G1 – PSoS have a page on their website titled 'Digital Device Examination by Agreement'. This page is a useful repository for information relating to MPE, and links to documents such as the Digital Device Examination Principles, the DPN template, internal flow processes for MPE, the legal basis for MPE and the PSoS privacy notices.

G2 - PSoS have amended their process for MPE to include the requirement for investigating officers to complete a DPN form when a victim and/or witness device is obtained. A victim and/or witness receives a copy of the DPN form, which combines both the DPNa and DPNb (user information sheet). PSoS have tailored the user information sheet and have made it applicable to their own processes, however this currently does not include any DP related information, for example:

- the lawful basis for processing and the condition for sensitive processing under Part 3;
- how the personal data will be kept secure and how long it will be retained;
- information on data subjects individual rights.

Recommendation:

G2 – The information provided within the DPNb template issued by the NPCC is integral to data subjects being fully informed of their information rights. PSoS should update their own DPN to include the DP related information included within the DPNb template issued by the NPCC, including:

- the lawful basis for processing and condition for sensitive processing under Part 3;
- how PSoS will be keep personal data secure and how long they will retain it for;
- information on data subjects individual rights (including links to applicable privacy notices).

Sufficient privacy information for MPE will ensure data subjects are fully informed on how personal data is handled.

Accepted: Yes

Management Response: The template review is underway and will align with this recommendation.

Action owner: SIRO

Implementation date: 1 January 2024

Scope area: H. Limited Purpose

Findings:

H1 – Personal data obtained through the use of MPE is limited to a specified explicit and legitimate purpose. This is reflected within a number of PSoS internal documentation, including the DPIAs for both digital device examination and the use of the cyber kiosks, which both reference s.36 of the DPA18, and the Digital Device Examination Principles document which explains the legitimate purpose for examining digital devices, including mobile phones. During interviews, ICO Auditors were informed of the process in place if information pertaining to another crime is found during the use of the cyber kiosks or through the MPE process. An intelligence report will be produced, and an additional ERF must be completed specific to the additional crime which has been identified.

Scope area: I. Data Minimisation

Findings:

I1 – As mentioned previously, investigating officers are required to complete both an ERF and DPN when submitting a mobile device for extraction. These forms record the line of enquiry, justification for the strict necessity and proportionality of the processing; the specific extraction/search/analysis undertaken; consideration of the level of collateral intrusion and steps taken to mitigate it.

I2 - Both the ERF and the DPN go through a mandatory quality check with a supervisor prior to the request being accepted via the Cyber Gateway. During interviews, ICO Auditors were informed that in some instances the DPN is not being submitted. Whilst supervisors will chase the missing DPN form, the kiosk procedure and internet page for CIDF do not make reference to the requirement for investigating officers complete a DPN.

I3 – PSoS have begun to monitor the number of extraction requests that are rejected by the CIDF. If a request is rejected, they will provide feedback to the investigating officer which submitted the request. Since this procedure was implemented PSoS have seen the number of rejections begin to drop, which they say is due to a better understanding of how to fill in the forms to the correct standard.

I4 – During interviews, ICO Auditors were informed that due to limitations with technology, it is not always possible to filter extractions specifically to what has been requested by the investigating officer and as such, more personal data is being extracted than required for the purposes of the investigation. On completion of extraction, forensic analysists produce a report for the investigating officer which only includes the information they have requested. Any additional personal data extracted is held on a shared drive within the segregated forensic network, until the investigating officer is satisfied with what has been provided in the report. The extraction is then archived on the server, which is only accessible by staff working within CIDF, meaning extractions cannot be inappropriately accessed, reviewed or disseminated.

Recommendation:

I2 – PSoS should ensure that any policies and/or procedures and applicable intranet pages for MPE sufficiently detail the correct process, including the requirement to complete a DPN, submit this alongside the ERF and to provide a copy to the victim and/or witness.

Accepted: Yes

Management Response: PSOS are currently reviewing all policies and/or procedures and applicable intranet pages relating to MPE to ensure they sufficiently detail the correct process, including the requirement to complete a DPN, submit this alongside the ERF and to provide a copy to the victim and/or witness.

These are being prioritised and will be subject of phased implementation given the iterative nature of policy/procedural review, update and full implementation therefore will be achieved by the date indicated below.

Action owner: SIRO

Implementation date: 1 April 2024

Scope area: J. Accuracy

Findings:

J1 – During interviews, ICO Auditors were shown the Cyber Gateway and ERF. The ERF requires investigating officers to record whether the data subject is a suspect, victim or witness as required within s.38(3) of the DPA18. Within the overarching DPIA for personal data processed by CIDF, PSoS state that the data source is recorded on every occasion, and the device owner is recorded within the case management system.

J2 - During interviews, a discussion was had regarding PSoS ability to implement the standards set out in the Forensic Science Regulator's (FSR) COP. ICO Auditors were informed that current legislation in Scotland does not allow for the full implementation of these standards, however PSoS are in the process of implementing the ISO17025, the standards in which the FSR COP states digital forensic services must be accredited to. It is noted within a progress update to the ICO's regional office in Scotland that PSoS have appointed a Cybercrime Quality Assurance Manager and associated team to implement ISO17025, with a pre-assessment by UKAS taking place in summer 2023 for the Aberdeen DFU. The accreditation is due to be extended to the other DFUs across the organisation once full accreditation is achieved in Aberdeen.

Recommendation:

J2 - PSoS should keep the implementation of the standards set out in the FSR COP under review. Additionally, they should continue with the phased implementation of ISO17025 and work toward accreditation for the standard.

Accepted: Yes

Management Response: Whilst PSoS are not bound to comply legally with FSR COP, we do seek to align any best practice and the implementation of ISO17025 will take effect when the first hub receives ISO17025 accreditation in Q2 of the 2024 calendar year.

Action owner: SIRO

Implementation date: 1 June 2024

Scope area: K. Storage Limitation

Findings:

K1 – PSoS have an overarching Records Management Policy which is supported by the Record Retention Standard Operating Procedure (SOP). The Digital Device Examination Principles document states that any data recovered will be stored in compliance with the Record Retention SOP. The overarching DPIA for CIDF covers s.39 of the DPA18, and states that a review of how the CIDF adheres to PSoS's Records Retention SOP and DP legislation is required. Risk 4 within Part 2, section 7 of the DPIA covers this within more detail.

During interviews, ICO Auditors queried the review, retention and deletion (RRD) process for extracted personal data, including how long extractions are retained within the CIDF once a copy has been provided to the investigating officer. PSoS explained the legislative requirements within the Criminal Justice and Licensing (Scotland) Act 2010, specifically the requirement to retain all information obtained throughout the course of an investigation, including non-relevant information, so that it's relevancy can be kept under review. It is the role of the investigating officer to let CIDF know that extractions are no longer required to be retained i.e. once sentencing has taken place, and it is a Team Leader's responsibility to determine when information is deleted.

Scope area: L. Security

Findings:

L1 – CIDF has a segregated forensic network where extractions take place and personal data is stored, air gapped from the rest of the network to maintain security. On completion of extraction, depending on the size of the file investigating officers will either receive the extraction via email or a forensic analyst will transfer the file via encrypted USB to the network so it can be accessed. Access to the CIDF is restricted to authorised personnel via

the user swipe cards and pin codes. For the use of the kiosks, the kiosk operators have their own username and passwords to login to the kiosks. There is a kiosk security operating procedure and user agreement which kiosk operators are required to sign.

Scope area: M. Data Protection by Design and Default

Findings:

M1 – PSoS's DP SOP refers to the requirement to comply with s.37 of the DPA18 (data protection by design and default) and states that where *'a type of processing, in part the use of new technologies, is likely to result in a high risk to the rights and freedoms of a data subject then a DPIA must be completed'*. PSoS have completed an overarching DPIA for all data processed within CIDF and a bespoke DPIA for the use of the cyber kiosks.

Scope area: N. Data Protection Impact Assessment

Findings:

N1 – As mentioned previously, PSoS have completed an overarching DPIA for all data processed within CIDF and a bespoke DPIA for the use of the cyber kiosks. The DPIAs adequately covers the DP principles and assesses the risks associated with the processing activity, including documenting any mitigations to the risks identified, however no DPO advice has been recorded on the copies of the DPIAs provided.

Recommendation:

N1 – Please see recommendation **A4**. If an organisation has a DPO, seeking their advice is a required part of the DPIA process. The DPO's advice and recommendations should be recorded on the DPIA, including in instances where the organisation does not follow the DPO's advice, including a justification of that decision.

Accepted: Yes

Management Response: As per response to A4.

Action owner: SIRO

Implementation date: 1 April 2024

Scope area: O. Recording of Processing Activity

Findings:

O1 – In response to questions 20 and 21 in the DPO MPE project questionnaire:

'*Does your data mapping reflect the processing of personal data obtained from MPE?*' and '*Is MPE documented within Police Scotland's Record of Processing Activity (RoPA)?*'

PSoS answered '*No*' and '*Don't Know'* respectively. During interviews, ICO Auditors were informed that PSoS have an IAR, which they use as their RoPA, however it does not reflect the processing of personal data acquired through the use of MPE.

Recommendation:

O1 - Without a clear understanding of how personal data extracted from mobile devices flows into, through and out of the organisation, further activities such as the development of the IAR/RoPA and risk assessments may be based on inaccurate or incomplete information which would result in non-conformance of s.61 of the DPA18. If MPE is not documented a part of their IAR/RoPA, PSoS will be in breach of s.61 & 42 of the DPA18.

PSoS should complete data mapping of their information assets to ensure a clear understanding of how personal data flows into, through and out of organisation. These completed data maps should clearly reflect the process of MPE. On completion of data mapping, PSoS must ensure all processing activities, including MPE, are formally documented. The ICO has produced guidance on documentation.

Accepted: Yes

Management Response: Priority will be given to MPE processing map which is interdependent with recommendation A3.

The update of the IAR is included on the IA Roadmap for 23-24.

To further enable this work a postholder will be dedicated 100% for a temporary period of (up to 12 months) to:

1. Update the data held

2. Update the in-life processes

Action owner: SIRO

Implementation date: 1 May 2024

Scope area: P. Rape and Serious Sexual Offence

Findings:

P1 – As mentioned previously, in May 2022 the Information Commissioner published an Opinion titled "Who's Under Investigation? The processing of victim's personal data in rape and serious sexual offence investigations." This builds upon the foundations established through the ICO investigation into MPE, with the Commissioner making a number of additional recommendations which relate to the processing of personal data within RASSO investigations, including when personal data is acquired from victims' electronic devices and when requests are made to third party organisations. The auditing toolkit for the MPE project has been further developed to assess progress with the recommendations within this Opinion.

As mentioned previously PSoS and COPFS are joint-controllers for certain processing activities, including the use of MPE and the recovery of sensitive personal records from third party organisations. Prosecutors may instruct PSoS to obtain a digital device for examination, or further examine a digital device that has already been obtained during the course of the investigation, if there are reasonable grounds to believe that the device may contain relevant information. In addition, during the investigation of any serious offence allegations (which would include

allegations of RASSO) prosecutors may instruct PSoS to obtain sensitive personal records from third party organisations. These records may provide evidence which will strengthen the prosecution case or support the defence case. These records include:

- Medical (GP or hospital);
- Psychiatric or Psychological;
- Counselling;
- Social Work;
- Education;
- Employment.

In the majority of cases, it is COPFS who determines whether these records should be obtained. If COPFS decides that records should be recovered the police will be directed to: recover the records; assess them for relevancy; and submit the relevant sections of the records. The sensitive records policy details a six step approach which should be adopted when considering whether sensitive records should be recovered. Prior to interviews some documents relating to third party requests were submitted as evidence. Staff explained that when they are instructed to make requests, they follow the process as outlined COPFS sensitive records policy and use the template documents that COPFS provide.

Recommendation:

P1 – Due to the joint controller relationship between PSoS and COPFS with respect to MPE and sensitive records requests, the decision was made to extend the MPE project to include COPFS. The engagement has resulted in a number of recommendations that may impact the process followed by PSoS on instruction of COPFS. Both organisations should liaise with one another to ensure any applicable changes to the process are communicated and followed.

Additionally, PSoS should ensure the Opinion is reviewed and any applicable recommendations to their own internal processes for MPE and third party requests are implemented into operational practice.

Accepted: Yes

Management Response: A short life working group with relevant SME from both PSoS and COPFS will be stood up for the purposes of addressing the first part of this recommendation which has interdependencies with recommendation A3 of this report.

The RASSO opinion is being further reviewed and any outstanding recommendations that have not yet been addressed will be implemented into operational practice.

Action owner: SIRO

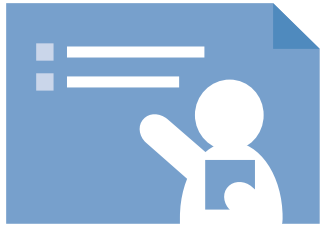
Implementation date: 1 May 2024.

Further reading

Information Commissioner calls for an end to the excessive collection of personal information from victims of rape and serious sexual assault. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2022/05/information-commissioner-calls-for-an-end-to-the-excessive-collection/

The call is published in a Commissioner's Opinion which informs the sector how to use victims' personal data in compliance with data protection laws.

Appendices



Appendix One –

Recommendations from the ICO investigation into mobile phone data extraction by police in the UK

Recommendation 1 – Roles and relationships

Police Scotland, the Crown Office and Procurator Fiscal Service and the Scottish Police Authority should jointly assess and clarify their mutual relationships and respective roles under the Data Protection Act 2018 in relation to law enforcement processing associated with criminal investigation. They should use the findings of this assessment as the basis for the review and revision of the governance and relevant policy documentation around MPE.

Recommendation 2 – Data protection impact assessment

Police Scotland should ensure it has DPIAs in place that cover all of its MPE operations, in order to demonstrate it understands and appropriately addresses the information risks associated with this practice. To ensure compliance with data protection requirements, Police Scotland should review and update such assessments prior to the procurement or roll-out of new hardware or software for MPE and processing, including any analytical capabilities. Where it identifies residual high risks associated with new processing, the force should undertake prior consultation with the ICO, as required under s65 of the DPA 2018.

Recommendation 3 – Standards and accreditation

In order to provide assurance around the integrity of the data extraction processes, Police Scotland should accelerate its work to implement and maintain the standards set out in the Forensic Science Regulator's codes of practice and conduct for forensic science providers and practitioners in the criminal justice system.

Recommendation 4 – Privacy information

Police Scotland should review and revise the information it provides to the public, including the range of documentation it publishes on its website and anything it provides directly to people during engagement. It should ensure that the documentation:

- adequately covers all processing arising from MPE;
- is consistent; and
- provides unambiguous information on privacy and information rights.

When considering this recommendation, the force should engage with, and may wish to adapt to their its circumstances, the work the NPCC is undertaking in relation to digital processing notices as a response to recommendation 2 of the England and Wales report.

Recommendation 5 – Data management

Police Scotland should review its data retention policy documentation and supplement it with materials to include:
- alignment of regular review and deletion processes across all operational, analytical and forensic environments; and
- processes to allow the separation and deletion of non-relevant material at the earliest opportunity, so that the force does not process it further and so officers cannot inappropriately access, review or disseminate the data.

Recommendation 6 – Consistency of approach

As far as legislative differences and devolved administration factors allow, Police Scotland should engage with work the UK Government, the NPCC and the College of Policing are undertaking. This work includes:

- the statutory power and code of practice being introduced through the Police, Crime, Sentencing and Courts Bill;
- police guidance on the considerations and processes involved in MPE; and
- privacy information officers provide to people whose devices are taken for examination.

Recommendations from the Information Commissioner published an Opinion titled Who's Under Investigation? The processing of victim's personal data in rape and serious sexual offence investigations

Recommendation 1 - The National Police Chiefs' Council must mandate to all police force/service(s) throughout the UK that they must cease using statements or forms indicating general consent to obtain third party materials (also known as Stafford statements – England and Wales). Data protection is not a barrier to fair and lawful sharing and acquisition, but data minimisation is key. Any personal data obtained relating to a victim must be adequate, relevant, not excessive and pertinent to an investigation.

Recommendation 2 - The Crown Prosecution Service, the Public Prosecution Service Northern Ireland and the Crown Office and Procurator Fiscal Service should ensure that their prosecutors are fully aware of this Commissioner's Opinion. They should be properly equipped to act according to the principles he promotes to uphold the rights and protections of victims.

Recommendation 3 - The National Police Chiefs' Council should work with the College of Policing and the Crown Prosecution Service to produce advice and supporting forms Information Commissioner's Opinion | 31 May 2022 49 for police force/service(s) to use across England and Wales when requesting personal information from third party organisations. The Police Service of Northern Ireland and Police Scotland should also work with the Public Prosecution Service Northern Ireland and the Crown Office and Procurator Fiscal Service respectively to produce similar documentation. The forms should be consistent with the principles established in this Commissioner's Opinion. They should:

- give clear advice to third parties who will be in receipt of such requests;
- make clear whether the requests are voluntary or mandatory:
- explain the reason for seeking the information: and
- explain that information sought might end up being disclosed to a defendant.

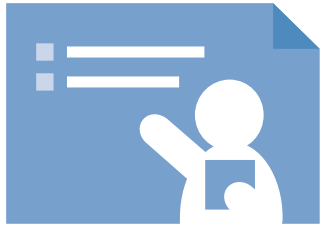
Recommendation 4 - The Commissioner makes further recommendations directly to the Chief Constables of forces across the UK, to ensure they are able to fully demonstrate compliance with data protection legislation when processing information relating to victims of rape and serious sexual offences (RASSO). Given the impact of investigators' interactions with the victims of RASSO cases, Chief Constables should update policy, guidance, training and other documentation to make it consistent with this Opinion. We expect this to cover at least the following areas:

- the circumstances under which it might be appropriate to seek access to material from (i) a victim's electronic devices, or (ii) other third party organisations. How they can use that information, who they can disclose it to, and how they can secure it;
- the formulation and documentation of appropriate parameters around material they are seeking;
- the nature of the contact with the victim and the information they should provide to them;
- the information they should provide to the third party organisation whom they are requesting material from; and
- how to deal with cases where a request for information is declined by a third party.

Recommendation 5 - Chief Constables across the UK must have in place appropriate policy, guidance and training for the ongoing management and retention of personal information relating to victims. This should ensure that they are managing and fully safeguarding information, whether they:

- obtain it directly from the victim;
- extract it from their devices; or
- acquire it from third parties. This is in accordance with this Opinion, the UK GDPR and the DPA 2018.

Credits



ICO Review Team

ICO Group Manager – Mandy Peach
ICO Team Manager – Eve Wright
ICO Senior Auditor – Grace Morgan

Thanks

The ICO would like to thank Richard Taylor, Detective Chief Inspector and Kerry Harvey, DPO, for their help with the MPE Project.

Distribution List

This report is for the attention of Richard Taylor and Kerry Harvey.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the engagement 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 the Police Service of Scotland.

We take all reasonable care to ensure that our 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 solely for the use of the Police Service of Scotland. The scope areas and controls covered have been tailored to this engagement and, as a result, the report is not intended to be used in comparison with other ICO reports.

Appendix B

POLICE SCOTLAND
POILEAS ALBA

ICO Mobile Phone Data Extraction Project

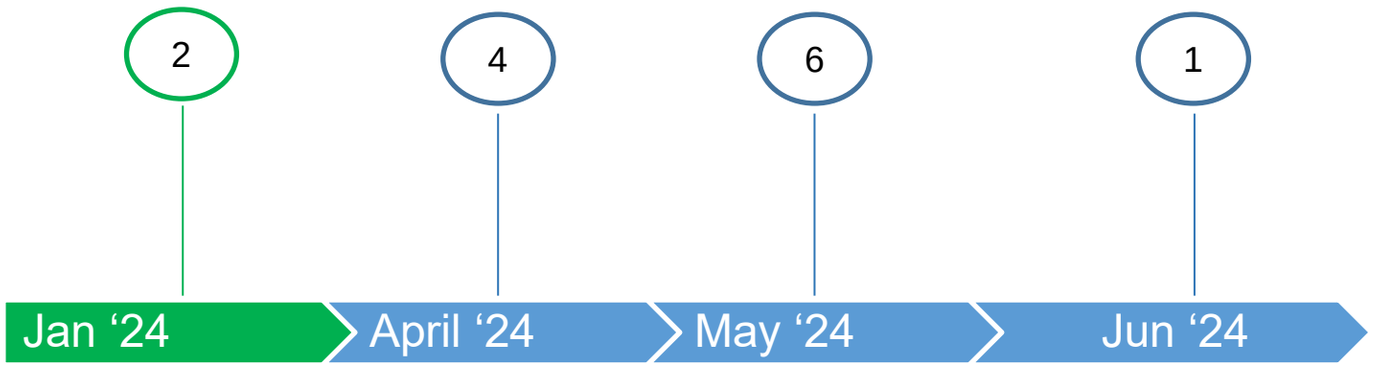
Police Scotland Review Report

Police Scotland Recommendations Dashboard

Total	Ongoing	Delayed	Closed to Date
13	13	0	**0**

Recommendations - Summary

- Ensure appropriate written agreements are in place with the Crown Office Procurator Fiscal Service (COPFS) for any processing activities where both parties are acting as joint data controllers.
- Review all policies and/or procedures relating to MPE which are accessible to staff, to ensure the content is up to date and follows the correct process, including the requirement to complete a DPN and provide a copy to victims and/or witnesses.
- Ensure any training on the use of MPE for investigating officers adequately covers the relevant DP requirements.
- Ensure the end to end process for MPE is captured within the Information Asset Register (IAR)/Record of Processing Activity (RoPA) to ensure the processing of personal data through the use of MPE is formally documented and risk assessed.



Challenges to delivery

Partner interdependencies
Resource and financial pressures
Consultation

ICO Mobile Phone Data Extraction Project 2023 - PSoS Recommendations				
Governance and Accountability Recommendations				
Number	**Rec Ref**	**Summary Title**	**Risk Rating**	**Target Date**
1	A3	Joint Controller Agreement - PSoS and COPFS	M	May-24
2	A4	DPIA Template Updates to Record DPO Advice	M	Apr-24
3	A6	Review Policies, Procedures & Guidance	M	Apr-24
4	C1	Create a separate APD for MPE processing	M	Jan-24
5	D1	Training on the use of MPE for investigating officers	M	May-24
6	E2	Programme of internal audit and/or compliance for MPE	M	May-24
7	F1	Promote the use of ‘agreement’ instead of ‘consent’	M	May-24
8	G2	Review and update Digital Processing Notice	M	Jan-24
9	I2	Update guidance with requirement to complete DPN and submit with ERF	M	Apr-24
10	J2	Keep standards set out in the FSR COP under review and continue with the phased implementation of ISO17025	M	Jun-24
11	N1	DPIA Template Updates to Record DPO Advice	M	Apr-24
12	O1	Complete data mapping for process of MPE (ROPA)	M	May-24
13	P1	Review of process followed by PSoS on instruction by COPFS	M	May-24

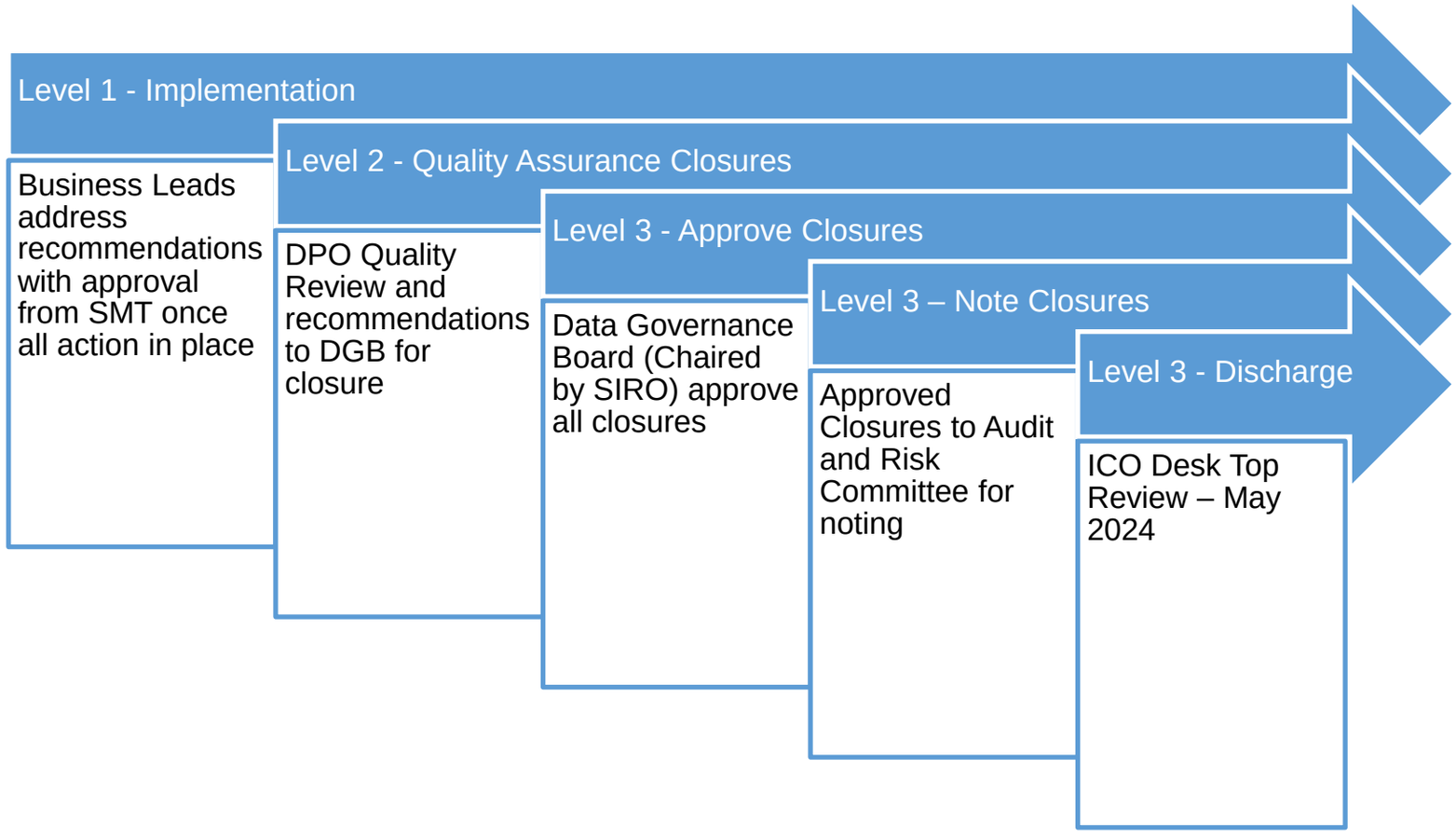
Police Scotland Recommendations – Progress

Total	Pending	Progressing	Delayed	Closed
13	2	11	**0**	**0**

- 11 Recommendations are in flight and on track.
- 2 Recommendations are pending which means the action is complete subject to publication date.

Report / Date	Recommendation	Risk	Date	Status
October 2023	A4 Governance & Accountability: DPO advice to be recorded on DPIA.	M	Jan 24	**Pending Evidence of Implementation** ICO acknowledges evidence of DPO advice recorded in communications with Digital Forensics. DPIA templates currently under review and once the new product is published, this can be closed.
October 2023	G2 Transparency: Update DPN to include Sufficient privacy information for MPE ensuring data subjects are fully informed on how personal data is handled.	M	Jan 24	**Pending Evidence of Implementation** A bespoke Privacy Information Notice and Appropriate Policy Document has been created for mobile phone digital extraction processing activities. Once published, this can be closed.

Governance



* All actions recorded in 4Action for effective management.