Findings from ICO reviews of mobile phone data extraction by police forces in the United Kingdom

Date issued: May 2024

Information Commissioner's Office

Contents

Introduction

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.

In June 2020, the ICO published reports into the practice of mobile phone data extraction (MPE) by police forces in England and Wales. These reports were published due to concerns that police forces were inconsistent in their approach to the handling of MPE, and that there were some poor practices in information handling including an overly wide approach to the extraction and processing of personal data from devices. Further reports covering Northern Ireland and Scotland were published in June 2021 along with an updated England and Wales report. The reports presented the findings from the investigation, as well as making recommendations to improve the consistency of police forces' approach to MPE.

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. 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 took the opportunity to update and expand our knowledge of how this activity is being undertaken within the sector.

Our approach

The first stage of this project commenced in March 2022. The ICO requested the completion of two questionnaires sent to Data Protection

Officers (DPO) and Operational Leads from police forces across the United Kingdom. The survey questions were developed based on the risks and recommendations from our investigation reports and additional data protection requirements applicable to MPE.

We received responses from 41 police forces which were subsequently assessed, and the responses were also used to develop the next stage of the project.

The second stage of the project commenced in July 2022. We approached nine police forces across the UK between July 2022 and September 2023 to take part in a more detailed review of their MPE practices.

The assessment criteria used for the reviews in this project were based on Part 3 DPA legislative requirements and designed to assess progress with the 13 recommendations and risks from the published report into MPE.

We produced individual reports for each participating police force, which detailed our review findings and provided additional and tailored recommendations to strengthen compliance.

As mentioned in the ICO investigation report there are three levels of MPE that could be performed.

- Level 1 – a logical extraction of data, involving a data kiosk[1] interacting with the device's own software;
- Level 2 – a physical extraction that could potentially retrieve deleted data or other data not accessible to the user;
- Level 3 – a full forensic specialist examination that may involve scientific examination of the device's physical components.

The focus of these reviews was primarily on level 1 extraction; however, we note that all three levels of extraction have their own distinct risk profile and should be managed effectively to ensure compliance with data protection legislation. This report should be read in conjunction with our earlier investigation reports for a comprehensive overview of MPE processing at each level of extraction.

[1] Kiosk is a 'self-service' device used by police forces to download and analyse the contents of individuals' mobile phones

Areas of improvement seen during reviews

As a result of our engagements with selected police forces, we noted several areas of good practice that featured in individual, or across several police forces:

Where 'informed agreement' of victims and witnesses is obtained when they provide their device to the police, the difference between that agreement and providing consent under DP law to process extracted personal data, is explained within relevant forms.

All requests for data extraction are triaged by a team with the appropriate training and knowledge and are rejected if the request does not meet the threshold. This process ensures that any submissions for extraction do not take place without forms being sufficiently detailed i.e. documenting the line of enquiry, the strict necessity and any alternatives to extraction which have been considered and rejected.

A process to monitor completion of the recommendations within the ICO investigation report on MPE is in place where actions taken to meet the recommendations are documented and progress RAG rated.

Some police forces have procured portable tablets that can extract material from mobile devices which has made the process more victim focussed. These tablets enable frontline officers to attend a victim/witness home address to conduct MPE, reducing the impact on the data subject by removing the need to travel to submit their device for extraction, minimising the time without their device and allowing victims/witnesses to observe the process.

Kiosks used for level 1 extraction showed that personal data is able to be extracted at a granular level. The kiosks can extract specific forms of data (i.e. SMS messages only) and data from particular apps, all within a specific date and timeframe. The system allows for extracted data to be 'tagged,' and anything that hasn't been tagged drops out of the system. Furthermore, the kiosks used allow for deletion once data is extracted and downloaded onto a removable device. The kiosk asks users to delete the information once extracted, and kiosks are cleansed weekly.

Key findings

By reviewing the responses we received to our surveys, and the subsequent individual reports created for the police forces that we reviewed we have identified reoccurring areas for improvement that were

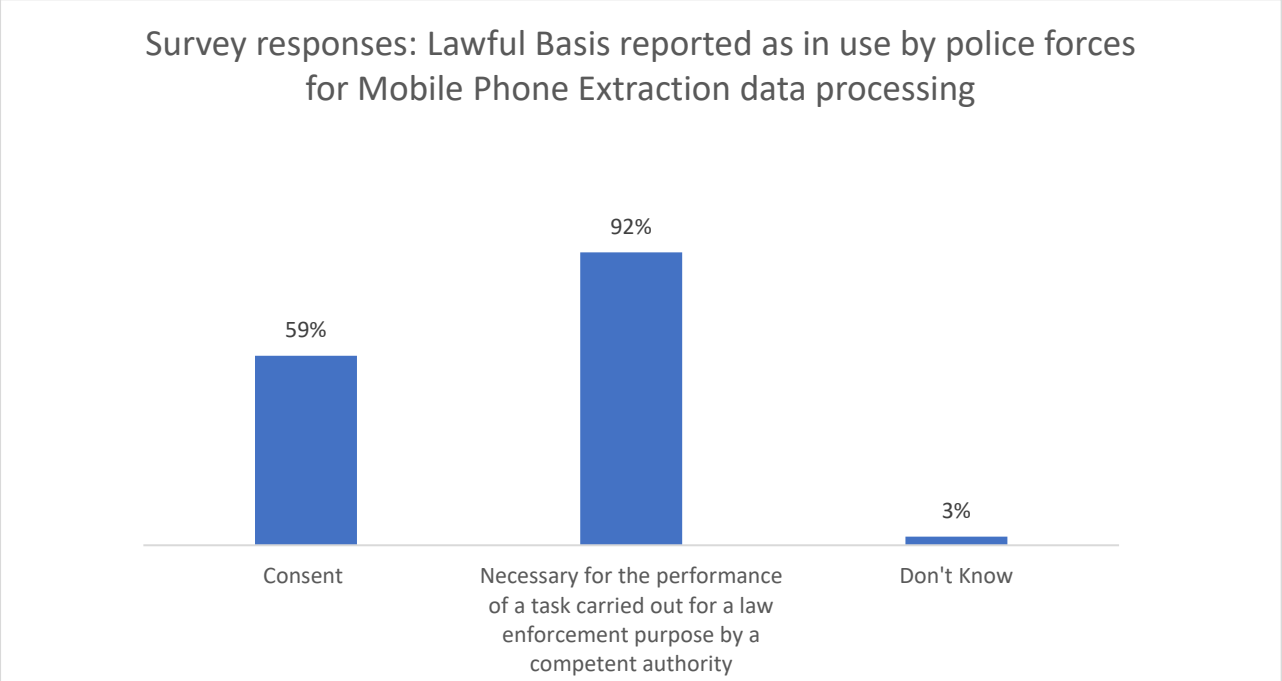
brought to the attention of our participants throughout our review. These areas relate to recommendations provided in our MPE investigation reports and additional data protection requirements relating to MPE. We have provided more detail on these areas below.

Data Protection Principles

Lawful and fair (the first data protection principle) – use of consent

What we found

The 2020 investigation report on the use of MPE by police forces in England and Wales focuses on the lawful basis police use to process personal data extracted from mobile phones. It stated that consent was often relied upon as the lawful basis for processing when the conditions for consent were not met, and that 'necessary for the performance of a task carried out for law enforcement purposes by a competent authority' would be more appropriate.



The initial survey responses from police forces indicated that the use of consent as a lawful basis for processing MPE data is still common, despite the ICO report recommending that it was not appropriate.

However, most of the police forces that were reviewed were not relying on consent as a lawful basis for MPE processing, although some were using the term consent to take possession of a device.

A lack of clarity in guidance for staff and the use of outdated forms to inform victims meant that there was still some confusion as to which lawful basis was being used.

What we have recommended

- Where consent is still being used as a lawful basis for the processing of personal data acquired by MPE this **should** be reassessed. Obtaining data solely with the device owner's consent is not likely to be an appropriate lawful basis, as that consent cannot always be withdrawn. The high standards required for consent to be valid could lead to non-compliance with section 35 of the DPA.
- Policies, guidance and training materials **should** be reviewed and updated to ensure the use of consent is clear, and investigating officers understand what lawful bases apply and when consent is and is not appropriate.
- MPE documentation and workflows **should** accurately reflect where consent is used and why. Eg consent may be used for taking possession of a personal device, while a different lawful basis applies to any information subsequently extracted from it.
- Police forces **should** ensure that staff are using the most up to date data processing notice (DPN) forms provided by the NPCC, including the forms used to inform data subjects. Any references to the forms in policies, procedures, guidance and training **should** be updated to ensure that the most up to date forms are being used. Inconsistent messaging regarding the use of consent for processing personal data may result in the incorrect lawful basis and condition for processing personal data being applied.

Specified, explicit and Limited purpose (the second data protection principle)

What we found

The police forces that had completed a data protection impact assessment (DPIA) for the MPE processing taking place could demonstrate that the risks relating to purpose limitation and had been identified and effectively mitigated.

However not all forces had completed a DPIA, and policies and procedures in place did not always document their approach to compliance with the purpose limitation principle.

What we have recommended

We recommended that police forces **should** document their approach to the purpose limitation principle in policies, procedures, training materials and guidance to ensure staff are aware of the requirements. Where a DPIA had not been completed for MPE forces were recommended to complete one as soon as possible.

Without ensuring that the purpose limitation principle is adhered to, personal data may be being processed in a manner that is incompatible with the purpose for which it was originally collected and could result in noncompliance with section 36 and the accountability principle of the DPA.

Adequate, relevant and not excessive (the third data protection principle)

What we found

DPN forms provided by the NPCC require police forces to document the necessity for the personal data to be extracted. These forms have been updated[2] and are kept under review. However, the updated forms were not always being used and some forces were still accepting out of date forms that don't contain sufficient information to demonstrate that the data being processed from devices was adequate, relevant, and not excessive.

Police forces that could demonstrate compliance with the data minimisation principle had processes in place to triage data extraction requests and rejected them where alternatives to extraction, which assisted in compliance with the data principle, had not been fully considered.

The software used by some forces allowed for targeted extraction using category filters to enable the extraction of specific forms of data. This capability was shown to limit the possibility of extracting data that is not relevant to an investigation.

What we have recommended

The need to use the latest version of DPN forms **should** be effectively communicated to staff, and outdated versions removed from circulation and rejected if used. Any policies and procedures, internet guidance and training materials that refer to these forms **should** also be routinely reviewed and updated as necessary to ensure the correct forms are in circulation. The use of outdated forms risks necessary information not

[2] As of the date of publication of this report, the latest DPNa and DPNb forms available from the NPCC are dated October and November 2022 respectively.

being recorded, specifically the consideration of the level of collateral intrusion and steps taken to mitigate it, which is missing from previous versions of these forms.

Police forces **should** review their current process for extracting material from mobile devices. This review **should** ascertain whether the technology used allows for targeted or specific data extraction. If limitations with technology mean that all data must be extracted to obtain what has been requested, processes **should** be put in place to abstract and delete nonrelevant personal data.

Accuracy (the fourth data protection principle)

What we found

Due to the specific risks identified in the earlier investigation reports, our reviews focused on assessing whether records created from the extracted data differentiated between categories of data subject (ie witness, victim or suspect). This is a specific requirement of section 38(3) of the DPA for all law enforcement processing. Most of the kiosks used for level one extraction did meet this requirement, and users were able to document whether the mobile device submitted for extraction belonged to a witness, victim or suspect.

However, we were unable to ascertain whether this was also the case when records were uploaded to the relevant case management system within wider networks.

What we recommended

Police forces **should** ensure when processing personal data for law enforcement purposes, a clear distinction **must**, where relevant and as far as possible, be made between personal data relating to different categories of data subject, such as victim, witness, suspect or offender. This applies to records created within the wider network as a result of an investigation involving data extracted from a mobile device. If there is no clear distinction made between the categories of data subjects, there is a risk that forces will be unable to establish the status of the data subjects that the personal data relates to, and non-conformance with section 38(3) of the DPA.

Storage Limitation - kept for no longer than is necessary (the fifth data protection principle)

What we found

Most police forces that participated in MPE reviews were unable to demonstrate that they had clear retention and deletion processes in place for personal data extracted through MPE. Some forces had recognised this as an issue and were developing measures to improve their review retention and disposal processes within the departments that were responsible for MPE. If appropriate and effective retention processes are not in place and implemented there is a risk of noncompliance with section 39 of the DPA.

What we recommended

Steps **should** be taken to review all DP related policies and procedures that refer to record retention and deletion processes to ensure they are in line with sectoral requirements and the current DP legislation. Policies and retention schedules **should** include MPE data and the relevant retention periods. This also applies to any personal data that is saved on removable media.

A review **should** take place to establish whether any existing MPE records (including any legacy data) should be retained or disposed of in-line with the retention policy. Key performance indicators (KPIs) **should** be in place to keep track of how many records are required to be reviewed, retained and disposed of. KPIs **should** be reported to senior management meetings to ensure oversight of compliance and assessment of risk.

Security (the sixth data protection principle)

What we found

The reviews we conducted focused on the security risks relating to the MPE process, namely the existence of appropriate access controls, kiosk configuration for encryption, transfer of downloaded data via removable media and authentication requirements of the systems used. Most forces were able to demonstrate that measures are in place to protect extracted data, but these requirements were not always documented in policies and procedures.

In one instance Kiosk Examiners had their own username and passwords, and once the data was extracted a report was produced which was encrypted with a standardised password. The force was unable to show that investigating officers were prompted to change this password to a more secure one on receipt of the data. During the review of another force ICO staff were made aware that some individuals were sharing passwords and were unable to ascertain if this was due to a lack of guidance or training.

If data is insecure due to insufficient technical and organisational measures this risks personal data breaches and noncompliance with section 40 of the DPA.

What we recommended

Police forces **should** ensure that passwords for systems used to process MPE personal data are secure to prevent inappropriate access or personal data breaches. If standard passwords are provided, then a process **should** be in place to ensure that the individual changes it to a more secure unique password.

Passwords and user accounts **should** only be given to officers and staff that have successfully completed the required security training before using MPE systems and regular internal reviews of kiosk user access **should** be taking place.

The technical and organisational measures in place to secure extracted personal data by level 1 kiosks **should** be documented within a relevant policy or procedure. This **should** cover access control, encryption, authentication requirements (eg, passwords) and the use of removable media to transfer personal data from the kiosks to the wider network.

Transparency (Information controllers' general duties) Section 34 DPA 2018.

What we found

Across the police forces that participated in the MPE reviews some weaknesses were identified in the privacy information made available to individuals, including victims involved in the MPE process, and in wider public facing privacy notices.

As noted in section 3 above, we encountered several police forces in our reviews that were using outdated DPN Forms when providing individuals subject to MPE processing with their privacy information. The latest DPNb form published by the NPCC provides important information to individuals subject to the MPE process, explains why their data is being processed and under what lawful basis, and their individual rights in relation to this processing.

It was also found that public facing privacy information did not reference or lacked detail regarding the processing of personal data for MPE.

What we recommended

Police forces **should** ensure they keep up to date with the latest guidance published by the NPCC and are using the latest DPN forms provided.

Public facing privacy notices **should** reflect the processing of personal data through the use of MPE and meet the requirements of section 44 (1) and (2) of the DPA.

Accountability and Governance

What we found

Responsibility and accountability for DP/information governance (IG) matters relating to MPE was not always clearly defined, including the roles of Senior Information Risk Owner (SIRO), DPO and oversight at Board meetings or steering groups.

A few of the police forces reviewed had policies and procedures in place that covered the process of MPE, however these tended to be focused on the technical aspects of extraction, rather than detailing the IG/DP requirements when using MPE technology within the organisation.

Sections 34 and 42 of the DPA18 require competent authorities[3] to have an appropriate policy document (APD) in place to ensure that the organisation has properly considered and documented their justification for sensitive processing[4]. Some of the police forces we reviewed did not have an APD in place for any of their sensitive processing. Most of the APDs that were in place did not provide enough detail about MPE data processing.

What we recommended

Police forces **should** ensure that there is effective and clearly defined oversight of MPE practice within the organisation. Responsibility and accountability for DP/IG related matters **should** be allocated to a Board of highest senior management level, ie the SIRO or equivalent. Responsibilities **should** be outlined in any policies and/or procedures for MPE. DP issues relating to MPE **should** be reported at Board meetings or Steering Groups. Police forces **should** also ensure that their DPO is adequately resourced and involved in the use of MPE.

As a minimum, the DPO **should** be reviewing policies, procedures and guidance, having input into training materials and the completion and

[3] Competent authority as defined under Schedule 7 of DPA 2018
[4] Sensitive processing as defined under Section 35(8) of DPA 2018

review of DPIAs for MPE. This will help to ensure that requirements are met and comply with the DPO task requirements of sections 70 and 71 of the DPA.

Where MPE processing is taking place forces **should** ensure that it has policies or procedures which sufficiently detail the specific DP requirements, for example information security, records management, and lawful bases. This may form part of an overarching DP Policy or policy framework which details the process of MPE within the organisation. These policies, procedures and guidance relating to the process of submitting mobile devices for extraction **should** be made readily available to all relevant staff and be regularly reviewed and updated.

An APD **should** be in place to ensure they have fully considered and documented their justification for any sensitive processing which makes it clear that consent is not relied on as a lawful basis and/or condition for processing personal data extracted from mobile devices. Due to the complexity of data extraction and the sensitivity of the personal data being processed, police forces may wish to create a separate APD for MPE processing.

Information Risk

What we found

The police forces reviewed have information risk management processes, but it was not always clear that all information risks relating to MPE were being identified, assessed, documented and managed appropriately. Although we were informed that processes were in place to escalate MPE information risks there was a lack of evidence to show that this does take place.

What we recommended

Police forces **should** ensure that there is a process in place to identify, document and manage information risks relating to MPE. This **should** include a process of escalation to any relevant information management steering group, committee or equivalent. The process **should** be formally documented within any applicable policies and or procedures. If information risk management is not effective, there is no assurance that appropriate steps have been taken to prevent the misuse of personal data. Increasing the possibility of a personal data breach and noncompliance with sections 40 and 66 of the DPA18.

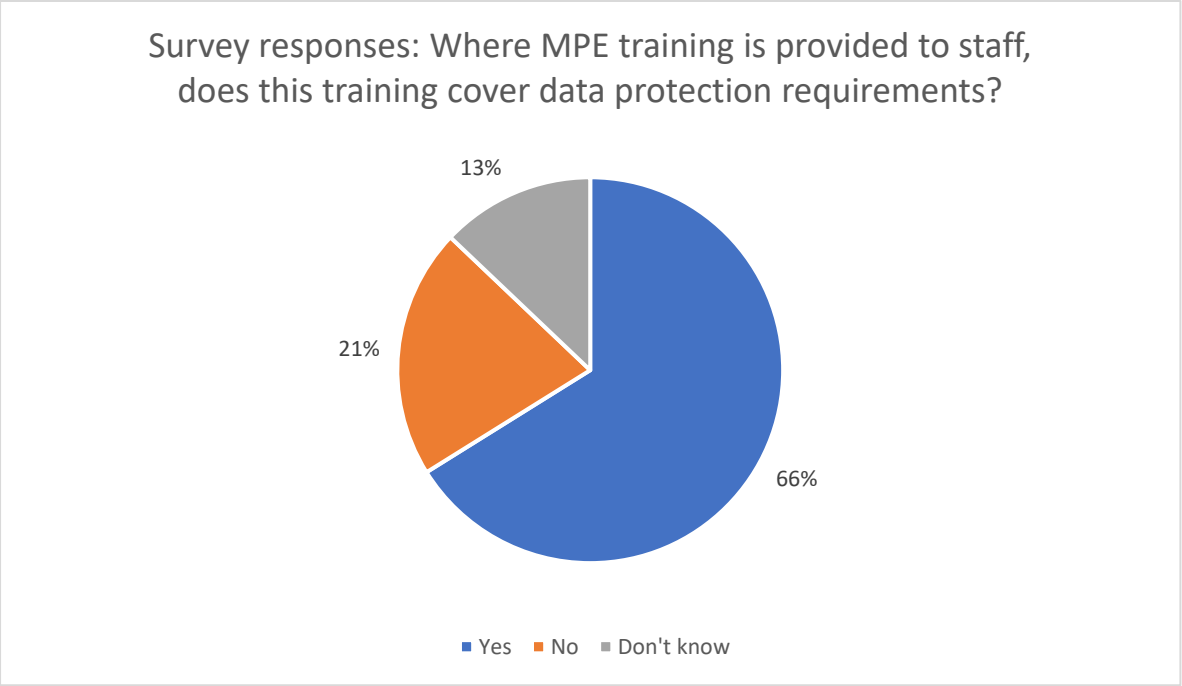
Training

What we found

The Home Office produced a Code of Practice, covering the extraction of information from electronic devices under the Police, Crime Sentencing and Courts Act 2022, in October 2022.

Recommendation nine of the report also suggested that a *"national training standard for all aspects of mobile phone extraction activity should be considered for investigating officers and decision makers to ensure consistency of approach."*

The ICO is aware that the NPCC and the College of Policing have collaborated to produce training content to support the code of practice.



Across the police forces that took part in MPE reviews, varying levels of training were reported to be provided to staff involved in MPE processing.

What we recommended

To ensure that staff involved in MPE processing receive sufficient training to understand the specific DP requirements and responsibilities for MPE. Police forces **should**:

- Include training on MPE in a training needs analysis and their overarching training programme. This will ensure all key roles and their relevant training requirements are identified and addressed.

- The DP training materials for MPE **should** sufficiently cover as a minimum:

  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 DP training for MPE **should** be refreshed as an appropriate frequency and reviewed regularly with staff being made aware of any changes to MPE processes and documentation eg when the NPCC DPN forms are updated.

Data Protection Compliance and Assurance

What we found

There was some evidence that police forces were undertaking or had undertaken elements of monitoring activity with respect to their MPE processing which included aspects of data protection compliance. However, most of the forces could not demonstrate that they had an agreed programme of risk based internal DP and IG reviews which included MPE. Without an extensive review programme which covers high risk processing activities such as MPE, organisations can have no assurance that their risk management is sufficient or effective.

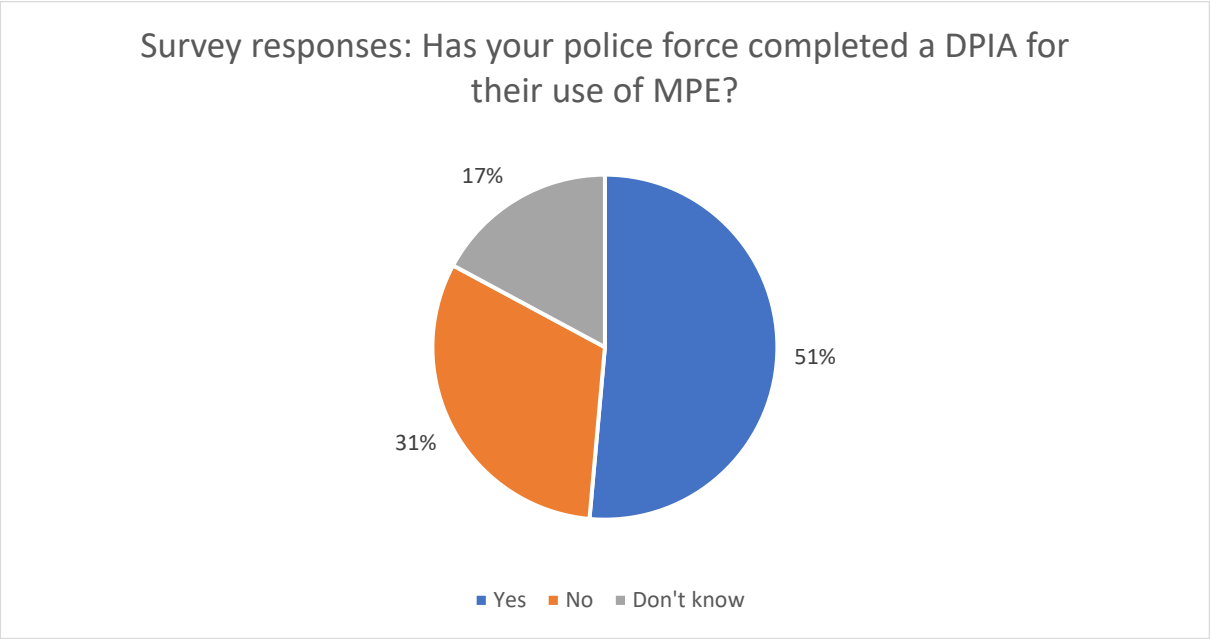
The lack of a sufficiently resourced review programme could result in nonconformance with sections 70 and 71 of the DPA18 and increase the risk of a data breach.

What we recommended

Police forces **should** ensure that they have a programme of regular internal reviews and, or compliance checks and **should** ensure the programme covers high risk processing activities such as MPE. This will help to gain assurance that applicable staff are following the correct procedures. Any reviews and, or compliance checks **should** adequately cover DP requirements.

Data protection impact assessments (DPIAs)

What we found



Our initial survey responses suggested that only half of police forces using MPE had completed a DPIA for this processing. It was noted across the majority of the police forces that took part in MPE reviews that DPIAs had not been completed for MPE processing activities, including any reviews to account for changes in the MPE process. A DPIA is a process to help identify and minimise the data protection risks of a project and **must** be completed for a DPIA for processing that is likely to result in a high risk to individuals.

What we recommended

We issued multiple recommendations in this area advising that;

- Where a DPIA had not been completed or finalised, police forces **should** complete one without further delay. This will help them to assess the information risks to this sensitive personal data and the rights and freedoms of individuals. The creation of a DPIA for MPE will help to identify and minimise the current DP risks, including an assessment as to whether the extraction of personal data complies with the principles of data minimisation and purpose limitation through the current process in place for extracting personal data from mobile devices.

- Police forces **should** act on the outputs of the DPIA to effectively mitigate or manage any risks identified to the personal data through the use of MPE hardware and software.
- The DPIA **should** be kept under review to ensure it remains up to date and compliant with requirements in section 64 and 65 of DPA18. If DPIA's are not reviewed periodically, new risks may emerge which are not identified and are left uncontrolled.

Data protection by design and default

What we found

Recommendation 10 in the ICO 2020 MPE investigation report included the requirement for a privacy by design and default approach, and the need to review software and build in privacy safeguards to any new procurement or upgrade.

The reviews considered the progress made towards meeting this requirement. If privacy safeguards are not in place from the outset of the extraction process, there is a risk that the rights of the individual are not adequately protected, and police forces may be in breach of the principles set out in sections 35 to 39 DPA.

It was reported across numerous police forces that limitations in MPE technologies meant that excess information was often collected from personal devices as it was not possible to target what data was extracted.

We did not observe any clear DP by design and default approach with respect to MPE practice, including whether privacy safeguards to any new procurement or upgrade of MPE hardware and software was routinely reviewed.

What we recommended

- Organisations using MPE technology **should** routinely review the hardware and software it uses to extract personal data from devices to ensure compliance with data protection legislation by design and default. This requirement **should** be integrated into any new procurement or upgrade of MPE hardware and software.
- Organisations **should** review the current process for extracting material from mobile devices to determine whether technology used allows for more targeted or specific data extraction to occur.
- Police forces that had not complete a DPIA for their MPE processes **should** do so as this will help them to identify and minimise the

current DP risks and assess their compliance with the principles of data minimisation and purpose limitation. DPIA's are an integral part of data protection by design and default.

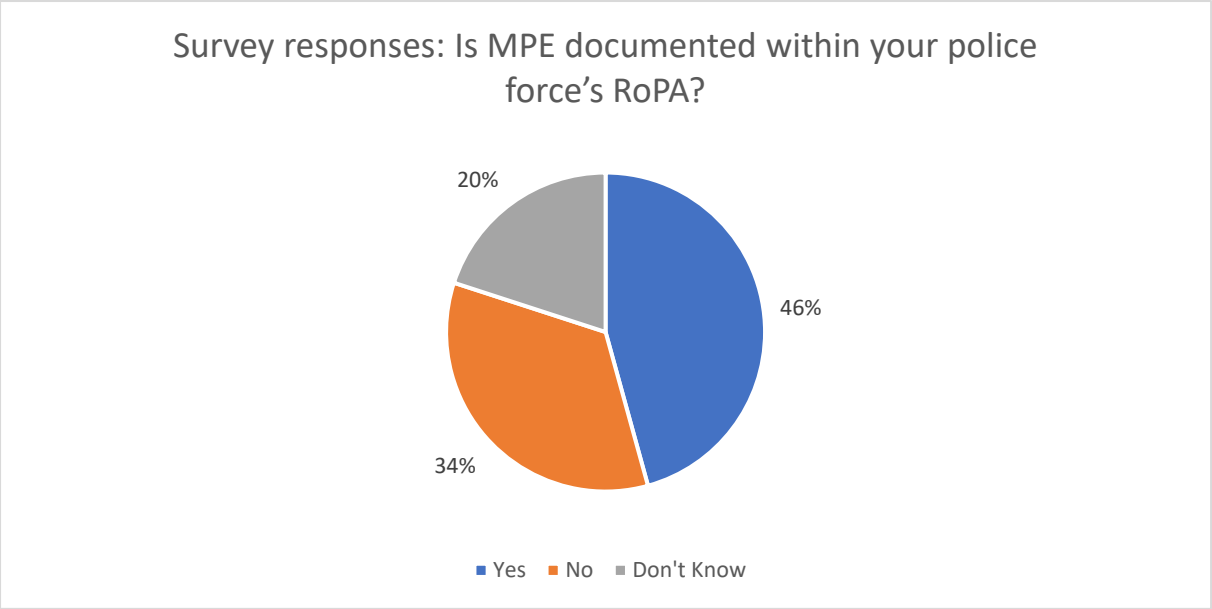
- Police forces **should** ensure that their approach to data protection by design and default is embedded into policies and procedures around the use of MPE.

Record of Processing Activities (RoPA)

What we found

Section 61 of the DPA requires competent authorities (including police forces) to keep records of all categories of processing activities involving personal data. This **should** include any personal data collected during MPE. It also helps to demonstrate compliance with the accountability requirements (section 34(3) DPA).

As well as being a legal requirement to document processing activities, recording what information is held, where it is and what is done with it makes it much easier to manage the data properly and keep it secure.



Our survey responses indicate that under half of police forces currently document MPE processing within their RoPA. Most of the police forces reviewed were unable to demonstrate that they had records of processing that sufficiently captured the MPE processing taking place. The majority of the RoPAs provided either did not include MPE or were not sufficiently detailed to meet statutory requirements.

What we recommended

- Police forces **must** ensure that they have a RoPA that documents all processing activities including MPE. The ICO has produced guidance and templates on documentation and Records of Processing Activities. They **should** ensure that entries on the RoPA for MPE contain all necessary information to comply with sections 42 & 61 of the DPA.
- To assist the development of a RoPA, police forces **should** ensure that MPE processing is reflected in their data mapping activity. This will ensure a clear understanding of how the personal data extracted from mobile devices flows into, through and out of the organisation and that further activities such as information asset registers and risk assessments are based on accurate and complete information. The results of data mapping **should** be regularly reviewed to ensure they remain accurate.

Follow Up Engagements

Each police force reviewed has received a detailed report of our findings, including recommendations to amend non-compliance or improve practice, where relevant.

In some cases, we decided that certain police forces would benefit from a follow up review so we could establish where action had been taken to improve compliance levels, and whether any further advice needed to be given to ensure that our recommendations were successfully implemented.

We have not found it necessary to take any regulatory action in relation to any of the participants we reviewed.

Acknowledgements

We'd like to thank the following police forces for their contribution to our review:
Avon and Somerset Constabulary
Bedfordshire Police
British Transport Police
Cambridgeshire Constabulary
Cheshire Constabulary
Cleveland Police
Derbyshire Constabulary
Devon & Cornwall Police
Dyfed-Powys Police
Durham Constabulary
Essex Police

Gloucestershire Constabulary
Greater Manchester Police
Gwent Police
Hampshire Constabulary
Hertfordshire Constabulary
Humberside Police
Kent Police
Lancashire Constabulary
Leicestershire Police
Lincolnshire Police
Merseyside Police
Metropolitan Police Service
Norfolk Constabulary
North Yorkshire Police
Northamptonshire Police
Northumbria Police
Nottinghamshire Police
Police Service of Northern Ireland
Police Service of Scotland
Suffolk Constabulary
South Wales Police
South Yorkshire Police
Staffordshire Police
Surrey Police
Sussex Police
Thames Valley Police
West Mercia Police
West Midlands Police
West Yorkshire Police
Wiltshire Police