Metropolitan Police Service Appropriate Policy Document Sensitive Processing for Law Enforcement Purposes

The Metropolitan Police Service ('the Met') is a police service established under the Police Act 1996.

The Met's Data Office can be contacted at: mpsdataoffice@met.police.uk.

As part of the Met's common law, statutory and corporate functions, we undertake sensitive processing for law enforcement purposes in accordance with the requirements of Part 3 and Schedule 8 of the Data Protection Act 2018 ('DPA 2018').

Definitions

Sensitive processing: defined in Section 35 (8) of DPA 2018 and is the processing of data equivalent to special category data detailed in the UK General Data Protection Regulations. This includes:

- Racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership.
- Genetic data, or biometric data.
- Data concerning health.
- Data concerning an individual's sex life or sexual orientation.

Law enforcement purposes: defined in Section 31 of DPA 2018 as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

What does this policy do?

This policy document explains the Met's procedures for securing compliance with the data protection principles outlined in Part 3 of DPA 2018, specifically in relation to sensitive processing for law enforcement purposes. It also explains the retention and erasure policies in relation to the sensitive processing. This policy is a requirement under Section 42 of DPA 2018.

Our policy document Metropolitan Police Service Appropriate Policy Document Processing Special Category and Criminal Offence Data explains our processing of special category and criminal offence data when our processing is not for the primary purpose of law enforcement.

This policy should be read in conjunction with the Met's Privacy Notice.

Description of data processed

As a police service it is necessary to carry out sensitive processing for law enforcement purpose to fulfil the functions of the Commissioner of Police of the Metropolis as both a competent authority defined under Section 30 of DPA 2018 and the responsible authority for the policing of the Metropolitan Police District.

We carry out sensitive processing of all of the categories of data defined in Part 3 Section 35 (8) of DPA 2018.

Section 35 (3) of DPA 2018 states that sensitive processing for a law enforcement purpose is permitted in only two cases:

i. the data subject has given consent to the processing for the specific purpose **and** at the time the processing is carried out, the controller has an appropriate policy document (APD) in place (Section 35(4)), OR;
ii. the processing is strictly necessary for a law enforcement purpose, the processing meets at least one condition in Schedule 8 of DPA 2018 **and** at the time the processing is carried out, the controller has an APD in place (Section 35(5)).

The Data Protection Principles

The principles set out in Chapter 2 Part 3 of DPA 2018 require personal data to be:

(a) Processed lawfully and fairly ('**lawful and fair**').

(b) Collected for specified, explicit and legitimate law enforcement purposes, and not further processed in a way which is incompatible with those purposes ('**specified, explicit and legitimate purposes**').

(c) Adequate, relevant and not excessive in relation to the purposes for which it is processed ('**adequate, relevant and not excessive**').

(d) Accurate, kept up to date where necessary and that every reasonable step is taken to ensure that inaccurate data is erased or rectified without delay ('**accurate and up to date where necessary**').

(e) Kept for no longer than is necessary for the purposes for which it is processed ('**kept for no longer than is necessary**').

(f) Processed in a way that ensures appropriate security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage ('**appropriate security**').

Section 34 (3) of DPA 2018 further adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, this Chapter" ('**accountability**').

Procedures for securing compliance with the Data Protection Principles:

1. Principle (a): lawful and fair

The Met will only undertake sensitive processing for a law enforcement purpose where it is lawful and fair, and:

- It is based on the consent of the data subject (as per section 35(4)), OR;
- It is strictly necessary for the law enforcement purpose, a Schedule 8 condition is met (as per Section 35(5)).

We communicate fair processing information to individuals through the Privacy Notice on the Met's Website and to individuals on request by contacting the Data Office via mpsdataoffice@met.police.uk. The information can also be provided in different formats if needed.

Where consent is requested from an individual to allow sensitive processing, the individual will be provided with full details of what will happen to their data and the length of time it will be retained. They will also be advised of the right to withdraw consent at any time before the information is processed. Where consent is requested, this information will be documented and available on request. In doing so, the Met will make sure the consent is unambiguous, given by an affirmative action and recorded as the condition for processing.

Where we do not rely on consent to process data, we ensure that the processing is strictly necessary for the law enforcement purpose(s) and that the processing meets at least one Schedule 8 condition.

The most common Schedule 8 condition which applies to law enforcement processing is:

- Condition 1 – Statutory or common law purposes.

The Met processes data as is necessary when exercising common law and/or statutory powers which includes but is not limited to powers under the Police and Criminal Evidence Act 1984, Criminal Procedure and Investigation Act 1996, the Protection of Freedoms Act 2012, Crime and Security Act 2010 and Immigration and Asylum Act 1999.

Other commonly used conditions are:

- Condition 3 – Protecting individual's vital interests; and
- Condition 4 – Safeguarding of children and of individuals at risk.

2. Principle (b): specified, explicit and legitimate purposes

The Met restricts sensitive processing to only that which is necessary for the relevant law enforcement purposes listed in Section 31 of DPA 2018, that is the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The Met will not further process personal data in a way that is incompatible with these purposes. Personal data gathered for one purpose may, however, be further processed for another law enforcement purpose by the Met or another organisation that is authorised to do so providing that the processing is necessary and proportionate to that purpose.

Personal data that has been collected for any of the law enforcement purposes will not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law (whether by statute or common law).

All officers and staff are made aware of the requirement that personal data can only be processed for an authorised law enforcement purpose in mandatory training, policies and operational notices.

3. Principle (c): adequate, relevant and not excessive

Any personal data collected for law enforcement purposes will be restricted to that which is necessary for the purposes of processing. The mandatory data protection training for all officers and staff emphasises that police records must ensure that personal data is adequate, relevant, unambiguous and professionally worded. Matters of opinion, which are not fact, will be clearly recorded as such. The information we process is necessary for and proportionate for us to carry out the policing purposes.

4. Principle (d): accurate and up to date where necessary

We, where relevant, and as far as possible, distinguish between personal data relating to different categories of data subject, such as:

- People suspected of committing an offence or being about to commit an offence
- People convicted of a criminal offence
- Known or suspected victims of a criminal offence
- Witnesses or other people with information about offences

This is evidenced by the Met's crime reporting information system which identifies and distinguishes between categories of data subjects such as victims, suspects and witnesses etc.

We will ensure as far as possible that the data we hold is accurate and kept up to date. In some circumstances we may need to keep factually inaccurate information e.g. in a statement from a victim, witness or alleged perpetrator. All officers and staff are made aware of the need for accuracy and are responsible for the accuracy of the personal data they process in mandatory training, policies and operational notices. Checks are carried out on the accuracy of data during audits and line manager checks. Personal data found to be inaccurate will be rectified or erased whenever possible. Where this is not possible, there will be an addendum to that personal data advising of the inaccuracy. Where appropriate, the processing will be restricted or data will be erased in accordance with Sections 46 to 48 of DPA 2018. This will ensure that relevant data will not be transmitted or otherwise made available.

If inaccurate personal data has been disclosed, the recipient will be advised of this as soon as practicable.

5. Principle (e): kept for no longer than is necessary

The Met has a Records Management, Retention and Disposal Policy which outlines the principles which the Met adhere to for the retention, review and disposal of records which have been created within its activities and functions. All sensitive processing will be dealt with under this Policy which is available on the internal Met website or following a request sent to the Data Office on mpsdataoffice@met.police.uk.

Data held on our systems is subject to scheduled and triggered reviews to ensure that information we hold on an individual is proportionate to meet the policing purpose(s). The Met has processes in place to deal with erasure requests submitted directly under the provisions of the DPA 2018, these are dealt with by the Met's Data Disputes Team.

For more information please contact mpsdataoffice@met.police.uk.

The Met also has processes in place to deal with early deletion requests that are submitted via ACRO pursuant to the provisions under the Protection of Freedom Act 2012, these are dealt with by the Met's Record Deletions Unit.

For more information please visit https://www.acro.police.uk/Record-deletion.

When an individual withdraws consent to the sensitive processing (where consent has previously been provided by the individual) that data will be destroyed in line with legislative requirements.

When sensitive processing is carried out in accordance with a Schedule 8 condition, the information will be retained or destroyed in accordance with the Met's Records Management, Retention and Disposal Policy.

6. Principle (f): appropriate security

The Met has developed and implemented appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Electronic and hard copy information processed for the law enforcement purposes is only available to officers and staff who carry out the processing for lawful purposes. Our electronic systems and physical storage have appropriate access controls applied.

Technical measures – The Met applies the information security standards set for the National Policing Community by the Cabinet Office and the Home Office. This includes encryption, firewalls, anti-virus software, IT health checks, vulnerability assessment and penetration process, user authentication, role based and password controlled access, technical assurance and technical audits and end point management.

Organisational measures - All officers and staff are required to undertake mandatory data protection training. All new staff, officers and contractors are vetted prior to being given access to the Met's information, systems and records.

Officers and staff receive training in how to use police systems before being granted access. Buildings are kept physically secure with access only being granted to individuals who require it.

7. Accountability Principle

The Met is responsible for compliance with the Data Protection Principles and in order to demonstrate compliance the Met will:

- ensure that records are kept of all personal data processing activities, and provide these records to the Information Commissioner's Office ('ICO') on request
- carry out a Data Protection Impact Assessment for any high risk personal data processing, and consult the ICO if appropriate
- ensure that a Data Protection Officer is appointed to provide independent advice and monitoring of the departments' personal data handling, and that this person has access to report to the highest management level of the department
- have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law
- take a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations
- implement appropriate security measures to protect all personal data held
- record and investigate all personal data breaches
- review and update our accountability measures at appropriate interval

Data controller's policies on retention and erasure of personal data

Where the Met no longer requires special category or criminal convictions personal data for the purpose for which it was collected, we will delete it or render it permanently anonymous. The Met's Records Management, Retention and Disposal Policy sets out the recommended time limits for erasure of the different categories of data.

The Met's Data Disputes Policy and Procedures sets out the handling of erasure and rectification requests received pursuant to your rights under DPA 2018. Erasure of personal data will be dealt with in accordance with Section 47 and (when necessary) Section 48 of DPA 2018. Rectification of personal data will be dealt with in accordance with Section 46 and (when necessary) Section 48 of DPA 2018. The Met's Privacy Notice explains your rights in relation to the erasure or rectification. A request for erasure or rectification can be made by contacting the Data Office on mpsdataoffice@met.police.uk.

Retention and review of this policy

This policy document will be retained in accordance with Section 42 of DPA 2018, and for the duration of our processing. It will be made available to the ICO on request.

The policy will be reviewed on an annual basis (or more regularly if circumstance requires) and updated as necessary at these reviews.

Further information

The Data Protection Officer can be contacted by email at: DataProtectionOfficer@met.police.uk

The Met Data Office manages the Met's data protection compliance and can be contacted at: mpsdataoffice@met.police.uk

Or, via post at: Met Data Office, PO Box 313, Sidcup, DA15 0HH