Metropolitan Police Service Appropriate Policy Document Processing Special Category and Criminal Offence Data

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 process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the UK General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Definitions

Special category data: defined in Article 9 UK GDPR as personal data revealing

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

Criminal offence data: defined in Article 10 UK GDPR as processing data in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing.

What does this policy do?

This policy document explains how the Met protects special category and criminal offence personal data relating to members of the public. This policy document also relates to the processing of MPS Employee/Contractor etc personal data, for the functions of the MPS as the Employer.

Article 9(1) UK GDPR prohibits the processing of special categories of data unless at least one condition in Article 9(2) is met. The Met must always ensure that its processing is generally lawful, fair and transparent and complies with all the other principles and requirements of the UK GDPR, which means it will need to identify an Article 6 lawful basis for processing, and, if processing special category data, also an Article 9(2) condition.

Article 9(2) UK GDPR has five conditions for processing provided solely in the UK GDPR, and five other conditions which require authorisation or a basis in UK law. These five conditions requiring authorisation in UK law are set out in the DPA 2018.

Article 10 of the UK GDPR sets out our legal authority for processing criminal convictions and offences and in accordance with the DPA 2018. While the Met sometimes processes criminal convictions data for non-law enforcement purposes, it will generally processes this type of personal data for the purposes of 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 ('Law Enforcement Purposes'). Our processing of special category and criminal offence data for law enforcement purposes is not covered in this document. Processing for law enforcement purposes is carried out by us in our capacity as a competent authority and falls under Part 3 of the DPA 2018. For further information please see the Met's Appropriate Policy Document on Sensitive Processing for Law Enforcement Purposes.

Some of the conditions for processing special category and criminal offence data in Schedule 1 DPA 2018 require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This document explains our processing of data to satisfy the requirements of Schedule 1 DPA 2018.

In addition it provides some further information about our processing of special category and criminal offence data where a policy document is not a specific requirement.

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

Conditions for processing special category and criminal offence data

The Met processes special categories of personal data under the following UK GDPR Articles:

(i) Article 9 (2) (a) – explicit consent.

In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

An example of our processing using explicit consent can be seen in parts of our recruitment process.

(ii) Article 9 (2) (b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Met or the data subject in connection with employment, social security or social protection.

Examples of our processing include staff sickness absences and processing data to discharge the Public Sector Equality Duty.

(iii) Article 9 (2) (c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.

An example of our processing would be using health information about an officer, member of staff or member of the public whose life is in danger and requires medical assistance.

(iv) Article 9 (2) (e) - where processing relates to personal data which are manifestly made public by the data subject.

An example of our processing would be if we drafted press lines relating to information that was placed into the public domain by a data subject.

(v) Article 9 (2) (f) – where processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

An example of our processing would be if our Directorate of Legal Services had to defend a legal claim brought against the Met.

(vi) Article 9 (2) (j) – where processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) (as supplemented by section 19 of the 2018 Act) based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

An example of our processing would be conducting research into trust and confidence in the Met.

(vii) Article 9 (2) (g) - where processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject domestic law.

An example of our processing would be engagement with monitoring groups to promote best practice in the Met and improve public trust and confidence. The Met is the largest police force in the United Kingdom and serves Greater London. It is in the substantial public interest that the Met has the public trust and confidence of the people whom it serves and thus must engage with the public, which may include processing special category and criminal convictions data.

Substantial Public Interest Conditions:

The Met relies on substantial public interest conditions in Part 2 Schedule 1 of DPA 2018 when processing personal data per the requirement of Article 9 (2) (g) described above.

As a police force, the Met satisfies this requirement by virtue of Paragraph 6: Statutory etc. and government purposes which is states that the condition is met if the processing:

- is necessary for reasons of substantial public interest (para 6(1)(b))
- is necessary for the exercise of a function conferred on a person by an enactment or rule of law (para 6(2)(a)); or
- is necessary for the exercise of a function of the Crown, a Minister of the Crown or a government department (para 6(2)(b)).

The Met's processing of data under Article 9(2)(g) may also be for one or more of the other twenty-two substantial public interest conditions listed in Part 2, in particular:

- Paragraph 7: Administration of justice and parliamentary purposes
- Paragraph 8: Equality of opportunity or treatment

- Paragraph 9: Racial and ethnic diversity at senior levels
- Paragraph 10: Preventing or detecting unlawful acts
- Paragraph 11: Protecting the public against dishonesty etc.
- Paragraph 12: Regulatory requirements relating to unlawful acts and dishonesty etc.
- Paragraph 13: Journalism etc. in connection with unlawful acts and dishonesty etc.
- Paragraph 14: Preventing fraud
- Paragraph 15: Suspicion of terrorist financing or money laundering
- Paragraph 16: Support for individuals with a particular disability or medical condition
- Paragraph 17: Counselling etc.
- Paragraph 18: Safeguarding of children and of individuals at risk
- Paragraph 19: Safeguarding of economic well-being of certain individuals
- Paragraph 20: Insurance
- Paragraph 21: Occupational pensions
- Paragraph 22: Political parties
- Paragraph 23: Elected representatives responding to requests
- Paragraph 24: Disclosure to elected representatives
- Paragraph 25: Informing elected representatives about prisoners
- Paragraph 26: Publication of legal judgments

The Data Protection Principles

The principles set out in Article 5 (1) UK GDPR requires personal data to be processed subject to the following principles that data must be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('**lawfulness, fairness and transparency**');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('**purpose limitation**');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('**storage limitation**');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**').

Article 5 (2) UK GDPR further adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability**')."

Procedures for securing compliance with the Data Protection Principles:

1. Principle (a): lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. The Met will:

- ensure that personal data is only processed where a lawful basis applies, and where processing is otherwise lawful
- only process personal data fairly, and will ensure that data subjects are not misled about the purposes of any processing
- ensure that data subjects receive full privacy information so that any processing of personal data is transparent

We will 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 this link mpsdataoffice@met.police.uk. The information can also be provided in different formats if needed.

To ensure that officers and staff adhere to the principle there is Met-wide internal mandatory training that is bolstered with policies that set the expectation that all staff and officers will abide by DPA 2018.

2. Principle (b): purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The Met will:

- only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice
- not use personal data for purposes that are incompatible with the purposes for which it was collected and if we do use personal data for a new purpose that is compatible, we will inform the data subject first

The Met has in place firewalls, systems and procedures to ensure that personal data is kept for the original purpose such as security firewalls and retention procedures.

3. Principle (c): data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The Met will only collect the minimum personal data required for the purpose for which it is collected and will ensure that the data we collect is adequate and relevant. The Met is committed to doing so by virtue of the fact data minimisation is incorporated into policies and procedures across the Met i.e. DPIAs, mandatory data protection training and data protection and retention policies.

4. Principle (d): accuracy

The Met will ensure that personal data is accurate, and kept up to date where necessary. 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.

If a data subject notifies the Met about an inaccuracy in personal data they will be referred to mpsdataoffice@met.police.uk. Personal data found to be inaccurate will then be rectified or erased whenever possible. Where this is not possible, an addendum can be added to that personal data advising of the inaccuracy. When necessary, the processing will be restricted in accordance with Sections 46 to 48 of the DPA. This will ensure that data will not be transmitted or made available for any of the law enforcement purposes.

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

5. Principle (e): storage limitation

The Met will only keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are collected and processed, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted or rendered permanently anonymous.

The Met has a Records Management, Retention and Disposal Policy that outlines the principles, the Met adhere to this 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.

6. Principle (f): integrity and confidentiality

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.

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 intervals

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 Retention 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 the Act. Rectification of personal data will be dealt with in accordance with Section 46 and (when necessary) Section 48 of the Act. 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 via this link mpsdataoffice@met.police.uk.

Retention and review of this policy

This policy document will be retained in accordance with Section 42 of the Act. 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