Greater Manchester Police Appropriate Policy Document

Sensitive Processing for Law Enforcement Purposes

Greater Manchester Police (GMP) is a Police Force established under the Police Act 1996. The GMP Information Compliance and Records Management Unit can be contacted at:

dataprotection@gmp.police.uk

What this Policy does

Part 3 of the Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing sensitive personal data for law enforcement purposes.

Sensitive processing is defined in Part 3 section 35(8) and is equivalent to UK GDPR special category data. This states that Sensitive Processing means:

- the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
- the processing of data concerning health;
- the processing of data concerning an individual's sex life or sexual orientation.

This Policy explains GMP procedures for securing compliance with the Data Protection principles listed below 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 the Data Protection Act 2018 (DPA).

Law enforcement purposes

"Law enforcement purposes" is defined 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.

As a Police Force it is necessary to carry out sensitive processing to fulfil the functions of the Chief Constable of Greater Manchester Police as both a competent authority and responsible for the policing of the GMP District.

Section 35(4) and (5) of the Act states that sensitive processing for law enforcement purposes is permitted in only two cases:

a) 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

or

b) The processing is strictly necessary for a law enforcement purpose, the processing meets at least one condition in Schedule 8 of the Act **and** at the time the processing is carried out, the controller has an APD in place.

If either of these two conditions are met, the sensitive processing will be lawful.

Compliance with Data Protection Principles

Section 34 DPA 2018 sets out the data protection principles which apply to the processing of personal data by a competent authority for a law enforcement purpose.

1. Processed lawfully and fairly (lawful and fair).

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

3. Adequate, relevant and not excessive in relation to the purposes for which it is processed (data minimisation).

4. Accurate and where necessary kept up to date (accuracy).

5. Kept for no longer than is necessary for the purposes for which it is processed (storage limitation).

6. 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 (integrity and confidentiality).

Accountability to the Principles

GMP has put in place appropriate technical and organisational measures to meet the requirements of accountability (as required by Section 34(3) DPA 2018). These include:

- The appointment of a Data Protection Officer (DPO) who has a key assurance, compliance and advisory role on data protection matters within the force;

- A direct reporting line from the DPO to our highest management level;

- The development and regular review of data protection policies and guidance for officers and staff setting how Greater Manchester Police meets its data protection obligations – such as when and how a Data Protection Impact Assessment (DPIA)

should be completed; and how to ensure new projects, applications or systems meet the legislative, technical and organisational requirements set out within UK data protection legislation;

- The appointment and training of Information Asset Owners (IAOs) to be responsible for the management of assigned information assets, including the identification and mitigation of risks arising from the processing of personal data, and ensuring the appropriate documentation is maintained for each of our processing activities;

- Implementing appropriate security measures in relation to the personal data we process by using guidance, and processes (such as the DPIA) to ensure officers and staff access to personal data and/or to systems containing such are limited and monitored; and

- Regularly reviewing of our accountability measures, and updating or amending them when required, and ensuring we take a 'data protection by design and default' approach to our activities, including the design of force systems.

Principle 1. Lawful and fair

GMP will only undertake sensitive processing where the processing is strictly necessary for the purposes of 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.

We will communicate fair processing information to individuals through the GMP website Privacy Notice 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.

Where the processing involves the taking or retaining of relevant physical data where the consent of the individual is not required, the legislation includes but may not be limited to; 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.

The Schedule 8 conditions which applies to GMP's law enforcement processing is:

- Condition 1 – Statutory purposes.
- Condition 2 – Administration of justice
- Condition 3 – Protecting individual's vital interests; and

- Condition 4 – Safeguarding of children and of individuals at risk.
- Condition 6 – Legal Claims
- Condition 8 – Preventing Fraud
- Condition 9 - Archiving

Principle 2. Specified, explicit and legitimate purposes

Sensitive processing will be restricted to only that which is necessary for the relevant law enforcement purpose and it will not be used for a matter which is not a law enforcement purpose unless that use is authorised by law. It may, however, be used for another law enforcement purpose by GMP or another organisation that is authorised to carry out law enforcement processing.

Principle 3. Adequate, relevant and not excessive

Any sensitive 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.

Principle 4. Accurate and where necessary kept up to date

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. 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. 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.

Principle 5. Kept for no longer than is necessary

GMP has a Retention and Disposal Policy which outlines the principles which GMP 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.

When an individual withdraws consent to the sensitive processing (where consent has previously been provided by the individual), that data may 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 Retention and Disposal Policy.

Principle 6. Appropriate security

GMP 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

Greater Manchester Police applies the information security standards set for the National Policing Community. This includes the use of encryption, firewalls, anti-virus software and user authentication. Technical assurance measures include IT health checks and other system auditing measures.

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 GMP'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.

Erasure of personal data

Erasure of Personal Data will be dealt with in accordance with Section 47 and (when necessary) Section 48 of the Act. See the Privacy Notice (Paragraph 12 within the Privacy Notice explains a data subjects rights in relation to the erasure or rectification. A request for erasure or rectification can be made by contacting the Information Compliance and Records Management Unit via dataprotection@gmp.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.