Appropriate Policy Document

Sensitive Processing for Law Enforcement Purposes

Who we are

The Police Service of Scotland (known as Police Scotland) is a police force established under Section 6 of the Police and Fire Reform (Scotland) Act 2012. Our headquarters are located at Tulliallan Castle, Kincardine, FK10 4BE.

What this policy does

This policy explains Police Scotland's 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 (the Act).

What is sensitive processing?

Sensitive processing is defined in Section 35(8) of the Act and means the processing of:

- personal data revealing 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

"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 as both a competent authority and responsible for the policing of Scotland.

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.

The Data Protection Principles

The principles set out in Part 3 of the Data Protection Act 2018 require personal data to be:

1. processed lawfully and fairly (lawfulness and fairness)
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).

How we will meet these principles in relation to sensitive processing

1. Lawful and fair

Police Scotland will only undertake sensitive processing for law enforcement purposes where it has a lawful basis to do so and where the information is required for a specific reason.

We will communicate fair processing information to individuals through the Police Scotland website and will also make the same information available on other formats to individuals on request.

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.

Should the processing involve the taking of relevant physical data, or samples as defined in section 18 of the Criminal Procedure (Scotland) Act 1995, action will be taken in accordance with Section 56 of the Criminal Justice (Scotland) Act 2003.

The most common Schedule 8 condition which applies to law enforcement processing is condition 1 – Statutory purposes. Other commonly used conditions are 3 – Protecting individual's vital interests and 4 – Safeguarding of children and of individuals at risk.

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 Police Scotland or another organisation that is authorised to carry out law enforcement processing.

3. 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 data protection training undergone by all officers and staff emphasises this. Officers and staff are also advised not to record their opinions unless that is a requirement

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 Act. 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. Kept for no longer than is necessary

Police Scotland has a Record Retention Standard Operating Procedure (SOP) which dictates the length of time personal data should be kept in certain circumstances. This SOP includes details of when the retention of personal data kept for specific purposes should be reviewed rather than destroyed. All sensitive processing will be dealt with under this SOP. The SOP is available on the force website.

When an individual withdraws consent to the sensitive processing (where consent has been previously requested and 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 / destroyed in accordance with the relevant section of the Record Retention SOP.

Should the sensitive processing based on consent involve the taking of relevant physical data, or samples as defined in section 18 of the Criminal Procedure (Scotland) Act 1995, action will be taken in accordance with Section 56 of the Criminal Justice (Scotland) Act 2003.

6. Appropriate security

Police Scotland 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

Police Scotland 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 appointment and must undergo training from Information Assurance and the Anti-Corruption Unit before being given access to Police Scotland systems.

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.

Further measures include the following SOPs:

- Data Protections
- Email and Internet Security
- Information Security Incident Reporting
- Information Security
- Information Sharing
- Mobile Data and Remote Working
- Record Retention
- Secure Destruction and Disposal of Data
- Storage of Records
- Vetting
- Visitors to Police Premises

7. 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.

8. 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 circumstances require it) and updated as necessary at these reviews.