Appropriate Policy Document

Processing of Special Categories of Personal Data and Criminal Convictions etc. (Non-Law Enforcement)

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 the processing of special categories of personal data. It also explains the retention and erasure policies in relation to that data. This policy is a requirement under Part 4 of Schedule 1 of the Data Protection Act 2018 (the Act).

What are special categories of personal data?

Special categories of personal data are:

- 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.

Article 9(1) of the GDPR prohibits the processing of special categories of personal data unless a specific condition in Article (9)(2) is met. In addition a condition in the Act, Schedule 1 Parts 1 or 2 must also be met.

Police Scotland's Privacy Notices set out the legal bases for processing the personal data held under both Articles 6 and 9 and the relevant Schedule 1 conditions.

Processing of personal data relating to criminal convictions etc.

As an official authority processing personal data in accordance with Article 6 of the GDPR, Police Scotland meets the requirements of GDPR Article 10 for the processing of personal data relating to criminal convictions etc.

The Data Protection Principles

The principles set out in the GDPR require personal data to be:

1. processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)
2. collected for specified, explicit and legitimate 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 they are processed (data minimisation)
4. accurate and where necessary kept up to date (accuracy)
5. kept in a form which permits identification for no longer than is necessary for the purposes for which the data are processed (storage limitation)
6. processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical and organisational measures (integrity and confidentiality).

The controller is responsible for and must be able to demonstrate compliance with the above (accountability).

How we meet these principles in relation to special categories of personal data

1. Lawful, fair and transparent

Police Scotland will communicate fair and transparent processing information to individuals using a range of methods, including provision of privacy notices, verbally, and posters which will be provided at the time the information is provided to us by the data subject.

The privacy notices are also on the Police Scotland Website. These notices detail the legal basis for processing types of special category data.

Posters are in all custody suites regarding the medical information which will be requested and the purpose for which it is required.

Where explicit consent is requested from an individual to allow processing of special category personal data, the individual will be provided with details of what special category personal data are involved, what they are consenting to (e.g. the sharing of their data), what will happen to their data and the length of time the data will be retained. They will also be advised of their right to withdraw consent at any time.

Where consent is requested, this information and the response from the individual will be documented and available for an audit trail.

2. Specified, explicit and legitimate purposes

Processing of special category personal data will be restricted to only that which is necessary for the relevant purpose and it will not be used for a matter which is incompatible with that purpose. Again, the privacy notices detail the purposes for which the personal data are processed.

If it is considered that further processing should be carried out (and that further processing is not based on consent), and the purpose does not fall within Schedule 2 Part 1, action will be

taken as per Article 6(4) of the GDPR to determine compatibility or otherwise of the proposed process. The result of this will be documented with the reasons for the decision.

If it is decided that the further processing is not incompatible with the original purpose, action will be taken as per Article 13(3) or Article 14(4) unless it is not appropriate, as per Article 13(4) or 14(5) respectively.

3. Adequate, relevant and not excessive

Any special category personal data processed 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 special category personal data we process are accurate and kept up to date. In some circumstances we may need to retain factually inaccurate information e.g. in job applications which do not represent the true facts.

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.

Special category personal data found to be inaccurate will be rectified or erased whenever possible. Where this is not possible at present due to the limitations of IT systems, there will be an addendum to that personal data advising of the inaccuracy. When relevant, the processing will be restricted in accordance with Article 18 of the GDPR.

Recipients of the relevant data will be notified of the erasure, rectification or restriction in accordance with Article 19 of the GDPR unless this proves impossible or involves disproportionate effort.

5. Kept in a form which permits identification of data subjects 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 details when the retention of personal data processed for specific purposes should be reviewed rather than destroyed. All processing of special category personal data will be dealt with under this SOP. The SOP is available on the force website.

When an individual withdraws consent to the processing of special category personal data (where consent has been previously requested and provided by the individual), that data will be destroyed on receipt of the withdrawal unless there is an overriding purpose for continued processing.

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 of all personal data processed.

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. Requests for erasure of special category personal data

Requests for erasure of special category personal data will be dealt with in accordance with Article 17 of the GDPR and when relevant, recipients of the relevant data will be notified of the erasure, in accordance with Article 19 of the GDPR unless this proves impossible or involves disproportionate effort. Any such decision will be recorded.

8. Retention and review of this policy

This policy document will be retained in accordance with Part 4 of Schedule 1 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.