Northamptonshire Police

Northamptonshire Police Appropriate Policy Document
Sensitive Processing for Law Enforcement Purposes
November 2020

Reference Number	30/20	Version	V1.0
Department Responsible	Information Assurance Unit		
Author	Trina Kightley-Jones C1278		
Senior Owner	Natalee Wignall X0223		
Effective Date	September 2020	GSC Marking	Official
Type	Policy		

Contents

Introduction

Northamptonshire Police is a 'competent authority' for law enforcement processing, as defined in Section 30 and Schedule 7 of the Data Protection Act 2018 (DPA 2018).

Part 3 of the DPA 2018 outlines the requirement for an Appropriate Policy Document (APD) to be in place when a competent authority is processing sensitive personal data for law enforcement purposes (LEP).

Sensitive processing is defined in Part 3, section 35(8) and is equivalent to GDPR special category data. This includes:

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

Processing for Law Enforcement Purposes must comply with the data protection principles outlined in Part 3 of the DPA 2018. Specifically, the first data protection principle (section 35) states that processing for Law Enforcement purposes must be lawful and fair.

Additionally, processing of sensitive personal data for Law Enforcement Purposes may only take place if the processing:

- is based on the consent of the data subject – section 35(4) **and** at the time when the processing is carried out, the Controller has an APD in place; **or**

- is strictly necessary for the specific law enforcement purpose and meets at least one of the conditions in Schedule 8 **and** at the time when the processing is carried out, the Controller has an APD in place – section 35(5)

This document demonstrates that the processing of sensitive data is compliant with the requirements of Part 3 section 42 of the DPA 2018. Section 42(2) specifies that for the above processing, the APD should:

a) explain procedures for securing compliance with the data protection principles in connection with sensitive processing in reliance on consent of the data subject *or* in reliance on the condition in question;
b) explains the controller's (Northamptonshire Police) policies as regards the retention and erasure of personal data processed in reliance on the consent of the data subject *or* in reliance on the condition in question, giving an indication of how long such personal data is likely to be retained.

Description of the Data Processed

Northamptonshire Police will process sensitive personal data where necessary for a law enforcement purpose – the law enforcement purposes are defined under section 31 of the DPA 2018 as 'The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security.'

It is likely that data processed by Northamptonshire Police in the course of our law enforcement functions will include all of the categories of sensitive personal data identified in Part 3, section 35(8) of the DPA 2018.

Lawful Basis

Consideration is required to ensure that consent provided by the data subject is an applicable basis for the processing of sensitive personal data for a law enforcement purposes by a Police Force. Where clear, explicit and unambiguous consent is not provided by the data subject, processing may be carried out for a law enforcement purpose and in reliance on one of the following Schedule 8 conditions of the DPA, including:

- Paragraph 1 – Statutory etc. Purposes
- Paragraph 2 – Administration of Justice
- Paragraph 3 – Protection of an Individual's Vital Interests
- Paragraph 4 – Safeguarding of Children and Individuals at Risk
- Paragraph 5 – Personal Data already in the Public Domain
- Paragraph 6 – Legal Claims
- Paragraph 7 – Judicial Acts
- Paragraph 8 – Preventing Fraud
- Paragraph 9 – Archiving etc.

Data Protection Principles

The principles set out in Part 3 of the DPA 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 minimization).
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 organization measures to protect against unauthorized or unlawful processing and against accidental loss, destruction or damage (integrity and confidentiality).

How we will meet these principles in relation to sensitive processing

Principle 1. Lawful and fair

The lawfulness of the sensitive processing carried out by Northamptonshire Police derives form our official functions as a Police Force.

Sensitive Processing will be carried out based on the explicit and unambiguous consent of the data subject or otherwise when necessary for a law enforcement purpose and in reliance on one of the Schedule 8 conditions detailed above.

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.

We will communicate fair processing information to individuals through the Northamptonshire Police website via our Privacy Notice and to individuals on request by contacting the Data Protection Officer. The information can also be provided in different formats if necessary.

Principle 2. Specified, explicit and legitimate purposes

Sensitive processing will be restricted to only that which is necessary for the relevant law enforcement purposes 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 Northamptonshire Police or another organization that is authorised to carry out law enforcement processing.

Principle 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 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 scheduled reviews. 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. The key law enforcement systems used by Northamptonshire Police make it possible to distinguish between sensitive data relating to different categories of data subject, where it is relevant to do so, 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

Principle 5. Kept for no longer than is necessary

Northamptonshire Police has a Records Management Review, Retention and Disposal Policy which outlines the principles which Northamptonshire Police adhere to for the retention, review and disposal of records which have been created within its activities and functions. Information processed by Northamptonshire Police will also be handled in accordance with College of Policing Authorised Professional Practice (APP) guidance on Management of Police Information (MoPI), which sets out the principles of good information handling practice. All sensitive processing carried out in accordance with a Schedule 8 condition will be retained or destroyed in accordance with the relevant section of our Policy and / or APP guidance on MoPI. This policy is available on the force website (pending) or sent direct on request to the Data Protection Officer.

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

Principle 6. Appropriate Security

Northamptonshire Police comply with the relevant parts of the legislation relating to security, and seek to comply with the College of Policing Information Assurance Authorised Professional Practice (APP), and relevant parts of the ISO27001 Information Security Standard.

Northamptonshire Police ensure that appropriate policy, training, technical and procedural measures are in place. These will include, but are not limited to, ensuring force buildings are secure and protected by adequate physical means. The areas restricted to police officers and force staff are only accessible by those holding the appropriate identification and having legitimate reasons for entry. Audits of our building security are carried out to ensure that they are secure. Northamptonshire Police standard operating procedures and policies make clear what use may be made of any sensitive data contained within them. Northamptonshire Police IT systems meet appropriate industry and government security standards.

All force staff are subject to pre-employment police vetting checks and periodical vetting checks once in post. All force staff have to undergo mandatory data protection and security training.

Any security incidents involving sensitive data are fully and corporately recorded, investigated and assessed for whether they should be reported to the Information Commissioners Office.

Retention and Erasure Policies

Northamptonshire Police has adopted the retention rules outlined in the College of Policing Authorised Professional Practice (APP) guidance on Management of Police Information (MoPI) and has in place record retention schedules which show how long records are retained.

We have Records Management policies which cover the principles of review, retention and disposal.

We also maintain an Information Asset Register and Record of Processing Activities that provide specific retention information for each information asset and processing activity within the Force. Access can be provided upon request. Please also see the Force Privacy Notice available here

Retention and Review of this Policy

This policy document will be retained in accordance with Section 42 of the DPA 2018. It will be made available to the ICO on request.

This policy will be reviewed on an annual basis (or more regularly if circumstances require it) and updated as necessary at these reviews.

Further Information

For further information about our compliance with data protection legislation or if you wish to contact our Data Protection Officer, please contact us using the details below:

Northamptonshire Police Data Protection Officer: Trina Kightley-Jones

Data Protection Officer
Northamptonshire Police Headquarters
Wootton Hall
Wootton Hall Park
Northampton
NN4 0JQ

Telephone: 03000 111 222
Email: dataprotection@northants.pnn.police.uk

Document Control History

DATE	VERSION	INDIVIDUAL	CHANGES MADE
19/11/20	1.0 (Draft)	Christian Kirkpatrick	First draft complete.
27/11/20	1.0 (Final)	Christian Kirkpatrick	Minor adjustments & watermark removed for publishing