Humberside Police

Serving our communities to make them safer and stronger

Appropriate Policy Document

Version 1.3

Last updated 24 January 2023

Contents

Introduction

Purpose

The purpose of this document is to enable the Humberside Police (Force) to meet the requirements set out in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018 for an appropriate policy document. This details the lawful basis and conditions for processing and safeguards the organisation have put in place when processing special category personal data.

This policy explains Force procedures for securing compliance with the data protection principles listed below in relation to special category data processing for law enforcement purposes. It also explains the retention and erasure policies in relation to this processing. This policy is a requirement under section 42 of the DPA 18.

This document demonstrates how the processing of this sensitive data is compliant with the requirements of Part 3 section 42 of the DPA 2018.

Scope

This Policy applies to all personal data, including special categories of personal data and Criminal Offence Data processed by the Force as defined under the UK GDPR and DPA 2018, including structured sets of personal data held in electronic or other filing systems that are accessible according to specified criteria. Additionally, this Policy applies to all data that is collected, created, processed, stored, transmitted (physically or electronically) or resides within information systems that are owned, operated, and managed by the Force.

Applicability

This Policy applies to all Police Officers and Police staff working for the Force (including those on secondment from other Government Departments and Agencies) as well as third parties acting on behalf of Force (e.g. temporary employees such as consultants, contractors, suppliers and resource company employees).

Policy

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 (LE) purposes.

Lawful basis for processing

For the purposes of fulfilling the role of a police service as defined under the Police Act 1996, the processing of personal data by the Force in the course of the exercise of its statutory Law Enforcement functions.

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 Commissioner of Police of Humberside as both a competent authority and responsible for the policing of Hull, East Riding and both North and North East Lincolnshire.

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.

Moreover, Article 6(1)(e) UK GDPR, when read with section 8 of the Data Protection Act 2018, provides a specific lawful basis for the processing of personal data by the Force, Article 6(1)(e) UK GDPR provides that:

- the processing of personal data shall be lawful where such processing is "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".

Special category and criminal conviction data

Special category data (defined by Article 9 of the UK GDPR) and sensitive data (defined by section 35 of the DPA 2018) is personal data which reveals:

- 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; and
- data concerning a natural person's sex life or sexual orientation.

Criminal Office Data covers a wide range of information about offenders or suspected offenders in the context of:

- criminal activity;
- allegations;
- investigations; and
- proceedings.

Conditions for processing special category data

The conditions which enable the processing of Special Categories of Personal Data under the UK GDPR are:

- Article 9(2)(g) - processing is necessary for reasons of substantial public interest; or
- Article 9(2)(i) - processing is necessary for reasons of public interest in the area of public health.

Substantial public interest

Section 10(3) of the DPA 2018 makes it clear that when it is necessary to process special categories of personal data for reasons of substantial public interest under Article 9(2)(g) of the UK GDPR, processing must meet one of the conditions set out in Part 2 of Schedule 1 DPA 2018.

In relation to the processing of special category personal data under Art.9(2)(g) by the Force, the substantial interest condition is met by virtue of paragraph 6 of Part 2 of Schedule 1 to the DPA 2018. It states that the condition is met if the processing:

- is necessary for reasons of substantial public interest (para 6(1)(b) of Schedule 1 DPA); and
- is necessary for the exercise of a function conferred on a person by an enactment or rule of law (para 6(2)(a) of Schedule 1 DPA); 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) of Schedule 1 DPA).

These conditions apply to the Force's functions. All processing is for the first listed purpose and might also be for others, depending on the context.

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
3. processed in a way which is incompatible with those purposes (purpose limitation)

4. adequate, relevant and not excessive in relation to the purposes for which it is processed (data minimisation)
5. accurate and where necessary kept up to date (accuracy)
6. kept for no longer than is necessary for the purposes for which it is processed (storage limitation)
7. processed in a way that ensures appropriate security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing

How Humberside Police will meet these principles in relation to sensitive processing

In accordance with the accountability principle, the Force maintains records of processing activities under Article 30 of the UK GDPR and section 61 of the DPA 2018. We carry out data protection impact assessments where appropriate in accordance with Articles 35 and 36 of the UK GDPR and section 64 of the DPA 2018 to ensure data protection by design and default.

The Force follows the data protection principles set out in Article 5 UK GDPR as follows:

Lawfulness, fairness and transparency

Lawfulness is explained in detailed in the preceding paragraphs. The Force will only undertake processing for law enforcement purposes where it has a lawful basis to do so and where the information is required for a specific reason. Transparency is essential for the Force to retain the trust of the public and to demonstrate the processing of personal data is undertaken in the correct manner. Privacy notices must therefore be available to the public and explain the nature and purpose of the processing and provide information about data subjects' rights using clear and plain language.

The Force will communicate fair processing information to individuals through the Force Privacy Notice. The information can also be provided in different formats if needed.

Where consent is requested from an individual to allow 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 most common Schedule 8 condition which applies to law enforcement processing is:

- Condition 1 – Statutory purposes.

Other commonly used conditions are:

- Condition 3 – Protecting individual's vital interests; and
- Condition 4 – Safeguarding of children and of individuals at risk.

Purpose limitation

The Force do not process personal data for purposes that are incompatible with the purposes for which it is collected. Special category 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 the Force or another organisation that is authorised to carry out law enforcement processing

When the Force share special category data or sensitive data with another controller or processor, we will ensure that the data transfers are compliant with relevant laws and regulations and use appropriate data sharing agreements and contracts.

Data minimisation

The Force shall collect personal data that is adequate, relevant and limited to the relevant purposes for which it is processed, and we ensure that the information we process is necessary and proportionate for its purposes. 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.

Accuracy

Personal data shall be accurate and, where necessary, kept up to date. Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay.

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.

Storage limitation

The Force has a Records Management, Retention and Disposal Policy which outlines the principles which the Force adhere to for the retention, review and disposal of records which have been created within its activities and functions. All special category processing will be dealt with under this Policy.

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

When special category processing is carried out in accordance with a Schedule 8 condition, the information will be retained or destroyed in accordance with the Records Management, Retention and Disposal Policy.

Integrity and confidentiality

The Force have put in place appropriate technical, physical and managerial procedures to safeguard and secure the information we collect about individuals. We have strict security standards, and all our staff who process personal data on our behalf receive regular training about how to keep information safe. We limit access to personal information to those employees, or third parties who have a business or legal need to access it.

Technical measures – the Force 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 Force'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.

Retention and erasure policies

Sensitive personal data processed for law enforcement purposes is held and disposed of in line with NPCC National Guidance on the minimum standards for the Retention and Disposal of Police Records, the College of Policing guidance on the Management of Police Information and Humberside Police Records Management Policy.

https://www.college.police.uk/app/information-management/management-police-information/retention-review-and-disposal

When disposing of information, the Force ensures this is carried out securely by using physical destruction methods as well as electronic data deletion.

Record of Processing Activities

In accordance with Part 4 of Schedule 1 of the Data Protection Act 2018, the Force maintains a record of processing activities under Article 30 UK GDPR. Amongst other things, this record includes information as to the processing condition that is being relied on, the lawful basis for such processing and whether the personal data is retained and erased in accordance with the Force's policies for the retention and erasure of personal data and, if not, the reasons for not following those policies.

Policy Review Statement

This policy will be periodically reviewed, at least annually and updated as necessary.

Last reviewed and updated on: 24 January 2023

Next scheduled review date: 25 August 2023