Data Protection Safeguards Policy

The processing of special and sensitive personal data for general and law enforcement purposes

Policy Reference: DP/APD

Approved: Information & Rish Governance Board – September 2002
Author: Rachel Walsh, Data Protection Officer
Produced: August 2020
Review due: August 2021
Last review: N/A
Review approved: (For reviewed procedures only): N/A

1. About this policy

The Data Protection Act 2018 (DPA) requires organisations to have a policy document in place when relying on certain lawful conditions to process sensitive, special category and some criminal offence data relating to people.

This policy explains the lawful conditions we rely on for both our law enforcement and non-law enforcement processes. It also outlines how we ensure this type of data is safeguarded in compliance with the DPA.

1.1 Special and sensitive data

Sensitive and special category data is defined as;

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

1.2 Law enforcement use

Where necessary, we can use any of the sensitive data categories when we exercise our law enforcement powers in respect of crime prevention, investigation, detection or prosecution. This includes safeguarding against, and prevention of, threats to public security. However, we only use what is necessary to achieve our purpose(s). This type of data is covered under Part 3 of the DPA. Further detail about the lawful conditions we rely on to do this are outlined at Section 2.

1.3 Non-law enforcement use

We process a wide variety of special data for non-law enforcement purposes, which can also include the use of criminal offence data. Again, we only use what is necessary to achieve our purpose(s). This type of data is commonly referred to as 'general processing' and is covered by the General Data Protection Regulation (GDPR) and Part 2 of the DPA. The lawful conditions we rely on to do this are outlined at Section 3.

1.4 Protecting special and sensitive data

We have a number of measures in place which help to demonstrate compliance of the DPA, GDPR and their Principles. Examples of these measures are outlined at Section 4.

2. Law enforcement purposes

We only process sensitive data where an individual consents or where it is strictly necessary for a law enforcement purpose in accordance with the following conditions:

2.1 Statutory purposes and the administration of justice

Any of the sensitive data categories can be used in order to fulfil our statutory duties relating to law enforcement and the administration of justice. For example, responding to emergency calls, managing high risk incidents, preventing, investigating and detecting crime, supporting the criminal justice system, as well as managing property and forensic material.

Examples of legislation can include; Criminal Procedure and Investigation Act 1996, Police (Conduct) Regulations 2020, Police and Criminal Evidence Act 1984.

2.2 Protecting individual's vital interests

Sensitive data categories can be used in order to protect individuals from serious harm. Examples include; preventing, investigating and detecting crime, managing high risk incidents as well as general incident deployment.

2.3 Safeguarding children and individuals at risk

Sensitive data categories can be used in order to safeguard children and vulnerable people. For example; during incident response and deployment, crime prevention, detection and investigation or internal conduct matters.

2.4 Personal data already in the public domain

Some of the information we use for law enforcement purposes is obtained through information which is already held in the public domain.

2.5 Legal claims

Sensitive data categories can be used during civil applications concurrent to criminal disposal. For example; under the Proceeds of Crime Act 2002 (POCA) and other criminal justice support.

2.6 Preventing fraud

Sensitive data categories can be used for the purposes of fraud prevention. This can include intelligence gathering and analysis.

2.7 Archiving etc.

We archive police data which includes sensitive data where it is in the public interest. We also use data where it is necessary for historical research and statistical purposes. Examples where we are likely to do this include; records relating to emergency response, custody and where race is captured within penalty notices for disorder. Other examples can include offender management and initial investigation.

3. General (GDPR) purposes

We only process special category and criminal offence data for general purposes to the extent that it meets a relevant lawful basis from the GDPR and where required, an additional lawful condition listed within the DPA. The relevant lawful conditions we rely on, which are required by this policy, are outlined below:

3.1 Employment, social security and social protection

Examples where we use special category data for employment purposes include; workforce planning, recording training, competency, injuries and risk management. It is also necessary for pension/payroll, salary deductions and employee relations purposes such as ill-health retirement, attendance cases and the occupational health process. In additional to special category data, criminal data can also be used for force vetting purposes.

3.2 Statutory purposes

The Asylum & Immigration Act 1996 requires us to assess eligibility to work in UK, which can reveal special category data during recruitment. The Police Regulations 2012 and Special Regulations 2015 also provide the framework for taking fingerprints from officers and staff.

Examples of other employment legislation which can result in the use of special category data include; Health & Safety at Work etc. Act 1974, the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR), the Diving at Work Regulations 1997, Trade Union and Labour Relations (Consolidation) Act 1992 and The Transfer of Undertakings (Protection of Employment) Regulations 2006.

Special category data can also be used for contingency planning purposes in accordance with the Civil Contingencies Act 2004, for firearms licensing matters (Firearms Act 1968 and subsequent Acts), for monitoring compliance with legal standards such as the DPA and GDPR, or where the Coroner needs to fulfil their duty under the Coroners Act 1988.

Moreover, special category data and/or criminal data can be used or shared in compliance with various legislation connected with the policing purposes. Examples include; Crime and Disorder Act 1998, Localism Act 2011, Digital Economy Act 2017, Police Reform and Social Responsibility Act 2011, Part 5 of Police Act 1997, Police (Property) Act 1897. A list of who we can share personal data with is listed within our privacy notice held on our website.

3.3 Administration of justice

Special category data can be used as part of a road-related matter where the outcome does not result in a criminal prosecution.

3.4 Equality of opportunity or treatment and racial and ethnic diversity at senior levels of organisations

We collect special category data and some criminal data for equality monitoring purposes. We also keep records of racial and ethnic diversity at senior levels of the organisation. However, we strive to collect this type of information anonymously.

3.5 Preventing or detecting unlawful acts

We use criminal information and/or special category data for the purpose of preventing or detecting unlawful acts. Examples include; the firearms licensing process, recording injuries and near misses, recruitment, vehicle recovery and whilst undertaking system monitoring.

3.6 Protecting the public against dishonesty

Criminal and/or special category data can be processed during recruitment and employee relations processes. This includes force vetting, dealing with complaints and internal conduct matters, elimination processes and whilst undertaking transaction monitoring. Where relevant and proportionate to protecting the public against dishonesty, we may publish this type of data through our internal communications.

3.7 Regulatory requirements relating to unlawful acts and dishonesty.

We use special category data and criminal information in order to comply with regulatory requirements in respect of complaints, internal conduct matters and statutory reviews.

3.8 Journalism etc. in connection with unlawful acts and dishonesty etc.

Criminal data will be shared or published where relevant and proportionate in respect of media enquiries (such as charging statements). We also engage production companies in line with this basis and in compliance with GDPR and other standards around television broadcasting. Some of the information shared may be derived from archived sources.

3.9 Safeguarding children and individuals at risk

We will process special category data, where necessary, to protect children and individuals at risk. This information could be collected or used in a wide-variety of situations such as; during police response, child protection meetings, adult and children referrals, offender management and through disclosures such as DBS and the courts.

3.10 Safeguarding economic well-being of certain individuals

We will process special category data during incident deployment situations where it is necessary to safeguard the economic wellbeing of individuals.

3.11 Insurance

We use some criminal and health-related information for insurance purposes related to court and criminal records disclosures and loss recovery.

3.12 Disclosure to elected representatives

MPs representing a constituent can request relevant information which can confirm criminal data. We rely on this condition to allow us to disclose the information required by them.

3.13 Publication of legal judgements

We rely on this condition when publishing the outcome of court results.

4. Complying with data protection

We have a number of measures in place which help to demonstrate compliance of the DPA, GDPR and their Principles. For example, we have a governance structure which includes a data protection officer, senior information risk owner (SIRO) and both an information compliance and information security team. We also report governance matters into an information risk governance board.

In addition, we undertake mandatory training, audit and monitoring as well as information security risk assessments and mandatory Data Protection Impact assessments (DPIAs). We also have appropriate information assurance policies which, together with key information messages, are sent directly to staff and tracked. Contractual and information sharing agreements are also in place.

We describe the Data Protection Principles and our procedures for complying with these below:

4.1 Principle 1 - ‘lawful, fair and transparent’

We ensure the processing is lawful and fair by identifying an appropriate lawful basis for its use and conduct DPIAs, where required, to consider the impact on people’s privacy. All processing of personal data, including sensitive, special and criminal data is documented within our Records of Processing Activity (RoPA).

Unless a DPA exemption or restriction applies, we will be open and honest when we collect sensitive, special category and criminal data. We also make privacy information available on our website and to individuals direct where relevant.

4.2 Principle 2 – ‘purpose limitation’

We are authorised to process personal data for a number of law enforcement and general purposes. We only re-use law enforcement data for a non-law enforcement purpose where authorised to do so by law and ensure any re-use of data is compatible with the original purpose collected. We achieve this through completion of DPIAs, information sharing agreements, mandatory data protection training and adhering to departmental procedures.

4.3 Principle 3 - ‘adequate, relevant and not excessive’

We only process sensitive and special category data where it is necessary and proportionate. We also anonymise or use pseudonyms were possible. We support compliance with this Principle by conducting DPIAs, completing training and ensuring appropriate access level controls are in place.

4.4 Principle 4 – ‘accurate and up to date’

Where we become aware of any personal data which is inaccurate or out of date, we take every reasonable step to ensure it is erased or rectified without delay. Where we decide not to erase or rectify, we document our decision.

We distinguish between the different categories of individuals for law enforcement processing and, as far as possible, distinguish fact from opinion.

We also take reasonable steps to ensure personal data is accurate before transmitting it. We do this by verifying data and providing recipients with necessary information to assess the accuracy, completeness and reliability of the data. If it becomes apparent that inaccurate data has been shared, we inform the recipient as soon as possible.

4.5 Principle 5 – 'kept for no longer than necessary'

The NPCC Minimum Retention Schedule outlines the minimum retention requirements for the records held by the Constabulary. We also provide an indication of any additional retention periods within our privacy notice held on our website.

4.6 Principle 6 – 'appropriate security'

We have a number of information assurance policies which provide a framework for ensuring personal data is adequately protected. Our electronic systems and physical storage have appropriate security, risk assessments, audit and access controls applied. We also have a process and procedure for recording personal data breaches and reporting them to the Information Commissioner's Office where necessary.

5. The Information Commissioner's Office

Regulation of the DPA and GDPR is the function of the Information Commissioner's Office (ICO). We fully co-operate with the ICO and make any relevant data available to them, without charge, which is required to perform its tasks.

This policy satisfies the requirements of Section 42, DPA (for law enforcement processing) and Part 4 of Schedule 1, DPA (for general processing). It is therefore an appropriate policy document in support of our compliance with the first data protection principle.

This policy will be reviewed annually or revised more frequently if necessary.