Law enforcement processing:

Part 3 Appropriate Policy Document

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 purposes.

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 LE 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. In addition, you may only process sensitive personal data for LE purposes if you have an APD, and if the processing:

- is based on the consent of the data subject - section 35(4);

  or

- is strictly necessary for the LE purpose and is based on a Schedule 8 condition - section 35(5).

The purpose of this document is to demonstrate 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 the procedures for securing compliance with the law enforcement data protection principles;

(b) explain the policies as regards the retention and erasure of personal data, giving an indication of how long the personal data is likely to be retained.

This document is a general policy for sensitive processing by the force. Where there are potentially high risks as a result of specific processing activities, a tailored policy document will be produced in respect of that activity, however this will be on an exceptional basis.

This APD must be kept under review and will need to retain it until six months after the date the relevant processing is stopped.

Description of data processed

Give a brief description of each category of sensitive data processed

- Racial or ethnic origin;
- Political opinions;
- Religious or other beliefs of a similar nature;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Offences and alleged offences;
- Criminal proceedings, outcomes and sentences;
- Cautions, reprimands and warnings;
- Physical identifiers, including DNA, fingerprints, and other genetic samples;
- Photograph, Sound and visual images;
- Criminal Intelligence;
- Information relating to safety;
- Incidents, and Accident details

Consent or Schedule 8 condition for processing

For the specific sensitive data you are processing for law enforcement purposes, explain whether you are relying on consent or a specific Schedule 8 condition for processing. Alternatively, you may wish to provide a link to your privacy policy, your record of processing or any other relevant documentation:

Statutory etc. purposes - is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and is necessary for reasons of substantial public interest

Administration of justice

Protecting individual's vital interests

Safeguarding of children and of individuals at risk - protecting an individual from neglect or physical, mental or emotional harm, or protecting the physical, mental or emotional well-being of an individual who is aged under 18, or aged 18 or over and at risk.
The processing is carried out without the consent of the data subject and the processing is necessary for reasons of substantial public interest.

- ☐ In the circumstances, consent to the processing cannot be given by the data subject;
- ☐ in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;
- ☐ the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection.
- ☐ "At risk" – An individual aged 18 & over is at risk if the controller has reasonable cause to suspect the individual has needs for care and support, is experiencing, or at risk of, neglect or physical, mental or emotional harm, and as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

Personal data already in the public domain – manifestly made public by data subject

Legal claims:

- ☐ necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
- ☐ necessary for the purpose of obtaining legal advice, or
- ☐ otherwise necessary for the purposes of establishing, exercising or defending legal rights

Preventing Fraud

☐ the disclosure of personal data by a competent authority as a member of an anti-fraud organisation,

☐ the disclosure of personal data by a competent authority in accordance with arrangements made by an anti-fraud organisation, or

☐ the processing of personal data disclosed as described above

Archiving etc

☐ for archiving purposes in the public interest,

☐ for scientific or historical research purposes, or

☐ for statistical purposes.

Procedures for ensuring compliance with the principles

You need to explain, in brief and with reference to the conditions relied upon, how your procedures ensure your compliance with the principles below.

This helps you meet your accountability obligations. You have a responsibility to demonstrate that your policies and procedures ensure your compliance with the wider requirements of Part 3 of the DPA 2018 and in particular the principles. The sensitivity of the data means the technical and organisational measures you have in place to protect it are crucially important.

In explaining your compliance with the principles, you should consider the specifics of your processing with respect to the specific data you have identified above.

There is also no requirement to reproduce information which is recorded elsewhere – **questions may be answered with a link or reference to other documentation, to your policies and procedures, your Data Protection Impact Assessments (DPIAs) or to your privacy notices.**

Accountability principle
i. Do we maintain appropriate documentation of our processing activities? Yes – Records of processing; logs; audits; DPIAs ii. Do we have appropriate data protection policies? Yes – there is an overarching data protection policy supported by guidance and process documents. There is also a suite of Information Security Policies.

iii. Do we keep logs in accordance with our obligations under section 62?

Yes, the operational systems are designed to meet the logging requirements.

Principle (1): lawfulness and fairness

i. If the processing is relying on a Schedule 8 condition, is the processing strictly necessary for the identified law enforcement purposes?

Yes – the processing will only take place where is a strictly necessary for the purposes of 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.

ii. If we are relying on consent for processing, are we satisfied that the consent is valid?

Consent is rarely used, however when it is it is freely given, fully informed, unambiguous and can be withdrawn at any time.

iii. Do we make appropriate privacy information available with respect to the sensitive data?

Yes. Information is available in the Privacy Notice and where required additional attention will be brought to it in the specific circumstances.

Privacy Notice | South Wales Police (south-wales.police.uk)

Privacy Notice | Gwent Police

Principle (2): purpose limitation

i. What are the law enforcement purpose(s) for processing as outlined in section 31?

the processing will only take place where is a strictly necessary for the purposes of 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

ii. Are our purposes for law enforcement processing specified, explicit and legitimate?

Yes.

iii. If we process sensitive data for a new law enforcement purpose, do we ensure the new processing is authorised by law and is necessary and proportionate?
Yes.

iv. If we are planning to use sensitive data for a new purpose other than law enforcement purposes, how will the processing be authorised by law and also meets the requirements of the GDPR and DPA 2018?
The compatibility test will be performed and consideration given to the fair processing information given at the time that the information was collected and whether additional information needs to be provided. As a statutory body, common law or statutory/regulatory powers will apply to all processing activities.

Principle (3): data minimisation

i. Are we satisfied that we only collect sensitive data we actually need for our specified purposes and that it is proportionate?
Yes – the systems are designed only to capture relevant information

ii. Are we satisfied that we have sufficient sensitive data to properly fulfil those purposes?
Yes – the systems are designed only to capture relevant information

iii. Do we periodically review this particular sensitive data, and delete anything we don't need?
Yes – there are specific review periods in place for all data.

Principle (4): accuracy

i. Do we have a process in place to identify when we need to keep the sensitive data updated to properly fulfil our purpose, and do we erase or rectify inaccurate data as necessary without delay?
Yes – although information may be marked with a supplementary statement instead of amendment where information cannot be changed for evidential purposes.

ii. Do we distinguish between sensitive personal data based on facts and sensitive personal data based on personal assessments (opinion)?
Yes.

iii. Where relevant and as far as possible, do we distinguish between sensitive personal data relating to different categories of data subject, as outlined in section 38(3)?
Each category of data subject is defined.

iv. Do we meet the verification requirements under section 38(5) for the transmission of data?
Yes.

Principle (5): storage limitation

i. Do we carefully consider how long we keep the sensitive data for the purpose for which it is processed and can we justify this amount of time?
Yes – all data is subject to review in accordance with retention periods

ii. Have we established appropriate time limits for the periodic review of the need for the continued storage of this sensitive personal data?
Yes – there are regulatory and statutory time limits for such periodic reviews.

Principle (6): security

i. Have we analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data?
Yes – data is assessed in a number of ways, DPIA, risk assessment, information risk assessment and information asset management, Data Protection compliance and is also subject to the Government Data Classification Scheme.

ii. Do we have an information security policy (or equivalent) regarding this sensitive data and do we take steps to make sure the policy is implemented? Is it regularly reviewed?
Sensitive data processed for law enforcement purposes is subject to regulatory and statutory requirements in terms of retention. There is an information security policy which addresses access controls and technical security measures and an overarching data protection policy which sets out the processing requirements for data.

iii. Have we put other technical measures or controls in place because of the circumstances and the type of sensitive data we are processing?
The information is kept on secure police systems. Users are vetted and access management is provided on a need-to-know basis. Training is provided annually to all staff and there is a dedicated Information Management Team which provides specific and general advice to the force on data handling matters. DPIAs are embedded into processes to ensure that appropriate measures are taken in respect of different types of data.

Retention and erasure policies

You need to explain your retention and erasure policies with respect to each category of sensitive data (this could include a link to your retention policy if you have one). You need to explicitly confirm how long you will retain each specific category of sensitive data, especially if the data no longer has any operational value.

Information is retained in accordance with the Management of Police Information, CPIA and PACE.

Non-operational data is retained in accordance with the force retention schedule.

APD review date

July 2022