Appropriate Policy Document

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category and criminal offence data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require you to have an APD in place. (See Schedule 1 paragraphs 1(1)(b) and 5).

This document should demonstrate that the processing of special category data and criminal offence data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles. In particular, it should outline your retention policies with respect to this data. (See Schedule 1 Part 4).

This document is a general policy for special category data and/or criminal offence data 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.

However if you rely on one of these conditions, your general record of processing activities under GDPR Article 30 must include:

(a) the condition which is relied upon;

(b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing); and
(c) whether the personal data is retained and erased in accordance with the retention policies outlined in this APD, and if not, the reasons why these policies have not been followed.

You must keep the APD under review and will need to retain it until six months after the date you stop the relevant processing.

Description of data processed

Give a brief description of each category of special category data/criminal offence data processed.

- Employment details;
- Financial details;
- Racial or ethnic origin;
- Political opinions;
- Religious or other beliefs of a similar nature;
- Physical or mental health 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

Schedule 1 condition for processing

Give the name and paragraph number of your relevant Schedule 1 condition(s) for processing. Alternatively, you may wish to provide a link to your privacy policy, your record of processing or any other relevant documentation:

- Privacy Notice | South Wales Police (south-wales.police.uk)
- Privacy Notice | Gwent Police
- The schedule 1 condition will depend on the specific circumstances.

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 the GDPR and in particular the principles. The sensitivity of SC and CO data means the technical and organisational measures you have in place to protect such data are crucially important.

The questions listed in each box are intended to help you describe how you satisfy each principle generally, and are based on the checklist for each principle provided in the Guide to the GDPR. They are not exhaustive and are only intended to act as a guideline.

In explaining your compliance with the principles you should consider the specifics of your processing with respect to the special category and criminal offence 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, Data Protection Impact Assessments (DPIAs) or to your privacy notices.**

Accountability principle

i. Do we maintain appropriate documentation of our processing activities?
Yes – there is a records of processing, DPIAs, contracts, audits, security testing etc.

ii. Do we have appropriate data protection policies?
Yes there is an overarching data protection policy which is supported by guidance and process documents.

iii. Do we carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests?
Yes – DPIA screening questions will be completed as best practice and DPIAs are embedded into processes with guidance to identify when they will be mandatory.

Principle (a): lawfulness, fairness and transparency

i. Have we identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing special category/criminal offence data?
Yes – this will depend on the specific circumstances.

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

Privacy Notice | Gwent Police

ii. Do we make appropriate privacy information available with respect to the special category/criminal offence data?
Yes – this information is provided in the privacy notice and also additional information is provided at the time that the information is collected where appropriate or necessary.

iii. Are we open and honest when we collect the special category/criminal offence data and do we ensure we do not deceive or mislead people about its use?
Yes – this is in accordance with the data protection requirements of transparency and the Police Code of Ethics.

Principle (b): purpose limitation

i. Have we clearly identified our purpose(s) for processing the special category/criminal offence data?

The need and purpose for this data is identified on a case by case basis

ii. Have we included appropriate details of these purposes in our privacy information for individuals?
Details are provided:

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

Privacy Notice | Gwent Police

iii. If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), do we check that this is compatible with our original purpose or get specific consent for the new purpose?
A compatibility test is conducted or additional fair processing information is provided. Where consent is used fresh consent will be collected.

Principle (c): data minimisation

i. Are we satisfied that we only collect special category/criminal offence personal data we actually need for our specified purposes?
Yes.

ii. Are we satisfied that we have sufficient special category/criminal offence data to properly fulfil those purposes?
Yes.

iii. Do we periodically review this particular special category/criminal offence data, and delete anything we don't need?
Yes – all data is subject to retention timelines and reviews.

Principle (d): accuracy

i. Do we have appropriate processes in place to check the accuracy of the special category/criminal offence data we collect, and do we record the source of that data?
Yes, where possible – although in some circumstances there is a legal obligation on the individual to provide accurate and correct information

ii. Do we have a process in place to identify when we need to keep the special category/criminal offence data updated to properly fulfil our purpose, and do

we update it as necessary?
Yes.

iii. Do we have a policy or set of procedures which outline how we keep records of mistakes and opinions, how we deal with challenges to the accuracy of data and how we ensure compliance with the individual's right to rectification?
Yes there is an overarching data protection policy with supporting guidance on individual rights.

Principle (e): storage limitation

i. Do we carefully consider how long we keep the special category/criminal offence data and can we justify this amount of time?
All data is subject to retention schedules/

ii. Do we regularly review our information and erase or anonymise this special category/criminal offence data when we no longer need it?
Yes – reviews are implemented within retention schedules.

iii. Have we clearly identified any special category/criminal offence data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes?
Yes – although this data is anonymised or pseudonymised where possible.

Principle (f): integrity and confidentiality (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 special category/criminal offence 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?

iv. 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 special category/criminal offence data (this could include a link to your retention policy if you have one). You need to explicitly indicate how long you are likely to retain each specific category of special category/criminal offence data.

Non-operational data containing personal information is retained in accordance with the force retention policy.

APD review date

July 2022