## ico_master_blue_rgb_Law enforcement processing: Part 3 Appropriate Policy Document template

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.

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

1. the processing of personal data revealing racial or ethnic origin,

political opinions, religious or philosophical beliefs or trade union

membership;

1. the processing of genetic data, or of biometric data, for the purpose of

uniquely identifying an individual;

1. the processing of data concerning health;
2. 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 LE 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).

This document should demonstrate that the processing of this 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:

1. explain your procedures for securing compliance with the LE data protection principles;
2. explain your policies as regards the retention and erasure of personal data, giving an indication of how long the personal data is likely to be retained.

If you conduct sensitive processing for a number of different LE purposes you do not need a separate policy document for each condition or processing activity – one document can cover them all. You may reference policies and procedures which are relevant to all the identified processing.

This Part 3 APD complements your general record of processing under section 61 in Part 3 of the DPA 2018 and provides any sensitive processing with further protection and accountability. See Part 3 section 42. Note section 42(4) outlines the obligations of data processors.

You must keep the APD under review and will need to retain it until six months after the date you stop the relevant processing. If the Commissioner asks to see it, you must provide it free of charge.

Note your APD does not have to be structured in accordance with this document. This template is intended as a guideline only.

|  |
| --- |
| Description of data processed |

Give a brief description of each category of sensitive data processed. You may wish to refer to your section 61 record of processing for that particular data:

|  |
| --- |
|  |

|  |
| --- |
| Consent or Schedule 8 condition for processing |

For the specific sensitive data you are processing for LE 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:

|  |
| --- |
|  |

|  |
| --- |
| 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.

The questions are intended to help you describe how you satisfy each principle

generally. They are not exhaustive and are only intended to act as a guideline. **The questions are broadly based on the requirements of each principle.**

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** |
| 1. Do we maintain appropriate documentation of our processing activities? 2. Do we have appropriate data protection policies? 3. Do we keep logs in accordance with our obligations under section 62? |
| **Principle (1): lawfulness and fairness** |
| 1. If the processing is relying on a Schedule 8 condition, is the processing strictly necessary for the identified LE purposes? 2. If we are relying on consent for processing, are we satisfied that the consent is valid? 3. Do we make appropriate privacy information available with respect to the sensitive data? |
| **Principle (2): purpose limitation** |
| 1. Have we clearly identified our LE purpose(s) for processing as outlined in section 31? 2. Are our purposes for LE processing specified, explicit and legitimate? 3. If we process sensitive data for a new LE purpose, do we ensure the new processing is authorised by law and is necessary and proportionate? 4. If we plan to use sensitive data for a new purpose other than LE purposes, do we check that the processing is authorised by law and also meets the requirements of the GDPR and DPA 2018? |
| **Principle (3): data minimisation** |
| 1. Are we satisfied that we only collect sensitive data we actually need for our specified purposes and that it is proportionate? 2. Are we satisfied that we have sufficient sensitive data to properly fulfil those purposes? 3. Do we periodically review this particular sensitive data, and delete anything we don’t need? |
| **Principle (4): accuracy** |
| 1. 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? 2. Do we distinguish between sensitive personal data based on facts and sensitive personal data based on personal assessments (opinion)? 3. 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)? 4. Do we meet the verification requirements under section 38(5) for the transmission of data? |
| **Principle (5): storage limitation** |
| 1. 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? 2. Have we established appropriate time limits for the periodic review of the need for the continued storage of this sensitive personal data? |
| **Principle (6): security** |
| 1. Have we analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data? 2. 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? 3. Have we put other technical measures or controls in place because of the circumstances and the type of sensitive data we are processing? |

|  |
| --- |
| 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.

|  |
| --- |
|  |

|  |
| --- |
| APD review date |

|  |
| --- |
|  |