|  |
| --- |
|  |
| ONR Policy  Appropriate Policy Document (APD) for special category and criminal offence data for law enforcement purposes |



ONR Policy

Appropriate Policy Document (APD) for special category and criminal offence data for law enforcement purposes

**Policy Owner**: Data Protection Officer (DPO)

**Prepared by** – Governance and Compliance Lead

**Approved by** – Data Protection Officer (DPO)

**Publication Date**: May 2024

**Next Major Review Date**: May 2027

**Issue No.:** 1

**Doc. Ref. No**.: ONR-DPC-POL-004

**Record Ref. No**.: 2024/27109

Revision Commentary

|  |  |
| --- | --- |
| Issue No. | Description of Update(s) |
| 1 | New policy document as part of our wider data protection compliance arrangements. |

Contents

[Introduction 4](#_Toc167190420)

[Purpose 4](#_Toc167190421)

[Scope and applicability 4](#_Toc167190422)

[Policy 5](#_Toc167190423)

[Description of data processed 5](#_Toc167190424)

[Consent or Schedule 8 condition for processing 5](#_Toc167190425)

[Procedures for ensuring compliance with the principles 5](#_Toc167190426)

[Accountability principle 5](#_Toc167190427)

[Principle (1): lawfulness and fairness 6](#_Toc167190428)

[Principle (2): purpose limitation 6](#_Toc167190429)

[Principle (3): data minimisation 7](#_Toc167190430)

[Principle (4): accuracy 7](#_Toc167190431)

[Principle (5): storage limitation 7](#_Toc167190432)

[Principle (6): security 8](#_Toc167190433)

[Retention and erasure policies 8](#_Toc167190434)

[Responsibilities 9](#_Toc167190435)

[Implementation 9](#_Toc167190436)

# Introduction

## Purpose

The [ONR Enforcement Policy Statement](https://www.onr.org.uk/documents/enforcement-policy-statement.pdf) describes ONR’s role in different areas and types of enforcement.

Where ONR processes information as a competent authority, Part 3 of the [Data Protection Act (DPA) 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) states the requirement for this Appropriate Policy Document (APD) to be in place when processing sensitive personal data for law enforcement purposes.

## Scope and applicability

As part of the ONR’s statutory functions, we can investigate and prosecute individuals and organisations for offences committed under the legislation we regulate, including the Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009. ONR is named as a competent authority for the purpose of Part 3 of the DPA 2018 which applies to the processing of personal data by such authorities for law enforcement purposes.

These purposes are set out at section 31 DPA 2018 and include the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, which might include the safeguarding against and the prevention of threats to public security.

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

* the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
* the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
* the processing of data concerning health;
* the processing of data concerning an individual’s sex life or sexual orientation.

Our policy for special category and criminal offence data explains our general processing, i.e., when the primary purpose is **not law enforcement**. This includes when ONR’s processing is in liaison with another competent authority such as the Police or Health & Safety Executive.

Additional information about our more general processing can also be found in our external and internal privacy notices.

# Policy

This policy outlines our sensitive processing for law enforcement purposes and explains:

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

## Description of data processed

We carry out sensitive processing for law enforcement purposes in three key areas:

1. Criminal investigations
2. Intelligence
3. Financial recovery

## Consent or Schedule 8 condition for processing

We carry out sensitive processing under section 35(3) DPA 2018 only in reliance on the consent of the data subject or where it is strictly necessary for the law enforcement purposes and it meets one of the conditions in schedule 8 of the DPA 2018.

The relevant schedule 8 condition for our processing is Schedule 8 paragraph 1 – statutory purposes.

Where personal data is retained as a public record to be transferred to The National Archives, our condition is Schedule 8 paragraph 9, the processing is necessary for archiving purposes in the public interest.

## Procedures for ensuring compliance with the principles

### Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

* The appointment of a data protection officer who reports directly to our highest management level.
* Taking a ‘data protection by design and by default’ approach to our activities.
* Maintaining documentation of our processing activities.
* Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
* Implementing appropriate security measures in relation to the personal data we process.
* Carrying out data protection impact assessments for our high risk processing.

### Principle (1): lawfulness and fairness

Processing for law enforcement must be lawful and fair. Sensitive processing is only permissible if it is:

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

or

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

Our processing of sensitive data for law enforcement purposes satisfies the first Schedule 8 condition that it is necessary for the exercise of a function conferred on ONR by the legislation for which we act as a regulator e.g. The Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009, and is necessary for reasons of substantial public interest.

In circumstances where we seek consent, we make sure:

* The consent is unambiguous
* The consent is given by an affirmative action
* The consent is recorded as the condition for processing

### Principle (2): purpose limitation

We process personal data for all of the law enforcement purposes listed at section 31 DPA 2018. These are the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, which might include the safeguarding against and the prevention of threats to public security.

We are authorised by law to carry out sensitive processing for any of these purposes. We may process personal data collected for one of these purposes (whether by us or another controller), for any of our other law enforcement purposes providing the processing is necessary and proportionate to that purpose.

We will only use data collected for a law enforcement purpose for purposes other than law enforcement where we are authorised by law to do so.

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.

### Principle (3): data minimisation

We do not systematically collect or harvest sensitive personal data for law enforcement purposes. The information we process is necessary for and proportionate to our purposes. It is processed in the context of us carrying out processes which enable us to meet our stated purposes for processing.

Where sensitive personal data is provided to us or obtained by us but is not relevant to our stated purposes, we will erase it.

### Principle (4): accuracy

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. If we decide not to either erase or rectify it, we will document our decision.

We, as far as possible, distinguish between personal data based on facts and personal data based on personal assessments or opinions and mark the file to reflect the distinction. There are circumstances where this is not possible.

We, where relevant, and as far as possible, distinguish between personal data relating to different categories of data subject, such as

* People suspected of committing an offence or being about to commit an offence
* People convicted of a criminal offence
* Known or suspected victims of a criminal offence
* Witnesses or other people with information about offences

We only do this where the personal data is relevant to the purpose being pursued.

We take reasonable steps to ensure that personal data which is inaccurate, incomplete or out of date is not transmitted or made available for any of the law enforcement purposes. We do this by verifying any data before sending it externally. We also provide the recipient with the necessary information we hold to assess the accuracy, completeness and reliability of the data.

If we discover, after transmission that the data was incorrect or should not have been transmitted, we will tell the recipient as soon as possible.

We document our decision to make personal data available for any of the law enforcement purposes.

### Principle (5): storage limitation

We have a corporate retention schedule and retain information processed for the purposes of law enforcement for 6 years from closure of the matter unless there is a legitimate reason to retain it for longer.

### Principle (6): security

Electronic information is processed within our secure network. Hard copy information is processed within our secure premises. Where it is necessary for us to share information with third parties we consider the technical or organisational security measures they have in place before allowing access or transmitting data.

Electronic and hard copy information processed for the law enforcement purposes is only available to staff who carry out the processing for these purposes. Our electronic systems and physical storage have appropriate access controls applied.

The systems we use to process personal data for law enforcement purposes allow us to update personal data at any point in time or apply a note indicating personal data has been updated. They also allow us to log the following information:

* Collection
* Alteration
* Consultation (access)
* Identity of person who accessed
* Disclosures
* Combination of records
* Erasure

## Retention and erasure policies

We have a [Business Classification and Retention Schedule](https://www.onr.org.uk/publications/corporate-publications/other-corporate-publications/policy/onr-business-classification-scheme-and-disposal-schedule/) which includes personal information processed for law enforcement purposes.

# Responsibilities

ONR’s Data Protection Officer is responsible for this policy.

ONR staff processing data for Law Enforcement purposes are responsible for adhering to this policy.

# Implementation

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed annually or revised more frequently if necessary, as per ICO requirements.