

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

# 

ONR Policy

Appropriate Policy Document (APD) for processing special category and criminal offence data

**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-005

**Record Ref. No**.: 2024/27110

Revision Commentary

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

Contents

[Introduction 4](#_Toc167192717)

[Purpose 4](#_Toc167192718)

[Scope and applicability 4](#_Toc167192719)

[Policy 5](#_Toc167192720)

[Conditions for processing 5](#_Toc167192721)

[Processing which requires an Appropriate Policy Document 6](#_Toc167192722)

[Description of data processed 6](#_Toc167192723)

[Schedule 1 conditions 6](#_Toc167192724)

[Procedures for securing compliance 7](#_Toc167192725)

[Principle 1 7](#_Toc167192726)

[Principle 2 8](#_Toc167192727)

[Principle 3 8](#_Toc167192728)

[Principle 4 8](#_Toc167192729)

[Principle 5 8](#_Toc167192730)

[Principle 6 9](#_Toc167192731)

[Accountability Principle 9](#_Toc167192732)

[Retention and disposal of personal data 9](#_Toc167192733)

[Responsibilities 10](#_Toc167192734)

[Implementation 10](#_Toc167192735)

# Introduction

## Purpose

Where ONR processes special category data relying on the conditions in Articles 9(2)(b), 9(2)(g) and 10 in the UK General Data Protection Regulation (GDPR), there is also a requirement in the Data Protection Act (DPA 2018) for ONR to implement appropriate safeguards for the fundamental rights and interests of the data subject.

Schedule 1, paragraph 1 of the DPA 2018 states that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

Schedule 1 paragraph 5 of the DPA 2018 states that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at of Schedule 1, paragraphs 6 to 28.

## Scope and applicability

This Appropriate Policy Document (APD) sets out how ONR will protect special category data and criminal offence data as defined in Schedule 1, Part 4 of the DPA 2018.

Our processing of special category and criminal offence data for law enforcement purposes is not covered in this document. Processing for law enforcement purposes is carried out by us in our capacity as a competent authority and falls under Part 3 of the DPA 2018. For further information please see our Safeguards Policy for sensitive law enforcement processing.

# Policy

## Conditions for processing

We process special categories of personal data under the following GDPR Articles:

i. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on ONR or the data subject in connection with employment, social security or social protection.

Examples of our processing include staff sickness absences.

ii. Article 9(2)(g) - reasons of substantial public interest.

ONR is the UK’s independent nuclear regulator for safety, security and safeguards.  We deliver five statutory purposes to ensure safe nuclear operations now and in the long term. These are:

* nuclear safety;
* nuclear site health and safety;
* nuclear security;
* nuclear safeguards; and
* safety of transport of nuclear and radioactive materials

Our processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role. Examples of our processing include the information we seek or receive as part of issuing licences and inspecting licensees.

iii. Article 9(2)(a) – explicit consent

In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing. Examples of our processing include dietary requirements and health information from visitors who require a reasonable adjustment to access our services.

iv. Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.

An example of our processing would be using health information about a member of staff in a medical emergency.

v. Article 9(2)(f) – for the establishment, exercise or defence of legal claims.

Examples of our processing include processing relating to any employment tribunal or other litigation.

vi. Article 9(2)(j) – for archiving purposes in the public interest.

An example of our processing is the transfers we make to the National Archives.

vii. We process criminal offence data under Article 10 of the UK GDPR.

Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations, and investigating potential crimes for reasons of substantial public interest under our duties as a regulator.

## Processing which requires an Appropriate Policy Document

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 an APD (see Schedule 1 paragraphs 1 and 5).

This policy demonstrates that the processing of special category and criminal offence data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. In particular, it outlines our retention policies with respect to this data.

## Description of data processed

We process the special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any trade union. Further information about this processing can be found in our [internal privacy notice](https://www.onr.org.uk/internal-privacy-notice.htm).

Our processing for reasons of substantial public interest relates to the data we receive or obtain in order to fulfil our statutory function as a regulator. This may be evidence provided to us as part of a complaint or intelligence information we gather for our investigations. Further information about this processing can be found in our external [privacy notice](https://www.onr.org.uk/privacy-cookies.htm).

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

## Schedule 1 conditions

**Special category data**

We process special category data for the following purposes in Part 1 of Schedule 1:

* **Paragraph 1(1)**employment, social security and social protection.

We process special category data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

* **Paragraph 6(1) and (2)(a)** statutory, etc. purposes
* **Paragraph 8(1)** equality of opportunity or treatment
* **Paragraph 10(1)** preventing or detecting unlawful acts
* **Paragraph 12(1) and (2)** regulatory requirements relating to unlawful acts and dishonesty

**Criminal offence data**

We process criminal offence data for the following purposes in parts 1 and 2 of Schedule 1

* **Paragraph 1** – employment, social security and social protection
* **Paragraph 6(2)(a)** – statutory, etc. purposes.

## Procedures for securing compliance

Article 5 of the GDPR sets out the data protection principles. These are our procedures for ensuring that we comply with them.

### Principle 1

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The personal data processed where this policy is required is only lawful if and to the extent it is based on law, and either the data subject has given their consent, or the processing meets at least one of the conditions in DPA 2018 Schedule 1.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notices, and this policy document.

Our processing for the purposes of employment relates to our obligations as an employer.

Our processing for purposes of substantial public interest is necessary for the exercise of a function conferred on ONR by the legislation for which we act as a regulator e.g., the Energy Act 2013.

We are the UK’s independent nuclear regulator for safety, security and safeguards. Our mission is to protect society by securing safe nuclear operations.

### Principle 2

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

ONR will:

A. Only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice; and

B. Not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, we will inform the data subject first.

### Principle 3

Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

ONR will:

A. Only collect the minimum personal data that we need for the purpose for which it is collected; and

B. Will ensure that the data we collect is adequate and relevant.

### Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

ONR will:

A. Ensure that personal data is accurate, and kept up to date where necessary; and

B. Will take particular care to do this where our use of the personal data has a significant impact on individuals.

### Principle 5

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

ONR will:

A. Only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so; and

B. Once we no longer need personal data it shall be deleted or rendered permanently anonymous in accordance with the ONR Business Classification Scheme and Disposal Schedule

### Principle 6

Electronic information is processed within our secure network. Hard copy information is processed in line with our security procedures.

Our electronic systems and physical storage have appropriate access controls applied.

The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

### Accountability Principle

ONR shall be responsible for, and be able to demonstrate, compliance with these principles. Our Data Protection Officer is responsible for ensuring that ONR is compliant with these principles.

We will:

A. Ensure that records are kept of all personal data processing activities (by means of a Personal Data Asset Register), and that these are provided to the Information Commissioner on request;

B. Carry out a Data Protection Impact Assessment for any high risk personal data processing, and consult the Information Commissioner if appropriate;

C. Ensure that a Data Protection Officer is appointed to provide independent advice and monitoring of personal data handling, and that this person has access to the highest management level; and

D. Have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law.

## Retention and disposal of personal data

Our retention and erasure practices are set out in our [Business Classification Scheme and Disposal Schedule](https://www.onr.org.uk/publications/corporate-publications/other-corporate-publications/policy/onr-business-classification-scheme-and-disposal-schedule/).

# Responsibilities

ONR staff processing special category data are responsible for adhering to this policy.

ONR’s Data Protection Officer is responsible for this policy. For further information, please contact us:

Office for Nuclear Regulation

Redgrave Court

Merton Road

Bootle,

L20 7HS

Email: [dataprotection@onr.gov.uk](mailto:dataprotection@onr.gov.uk)

# 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.