Annex A – DRAFT: Appropriate Policy Document

Data Protection Act 2018, Schedule 1
Appropriate Policy Document

Introduction

This policy has been developed to meet the Data Protection Act (DPA) 2018 requirement for an appropriate policy document which covers HSE's processing of special category and criminal offence data in accordance with the requirements of Article 9 and 10 of the UK General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Purpose

Its purpose is to explain what special category personal data is processed by HSE, the various reasons for which we use this data, and how we ensure it is handled in accordance with the core data protection principles set out in UK GDPR Article 5.

Definitions and Scope

Special category data (defined by Article 9 of the UK GDPR) is personal data which reveals:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

Sensitive Processing (defined by section 35 of the DPA 2018) is the processing of:

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

Article 10 UK GDPR covers processing in relation to criminal convictions and offences or related security measures. Section 11(2) of the DPA 2018 states that criminal conviction data includes data which relates to the alleged commission of offences and related proceedings and sentencing.

Conditions

HSE is an executive non-departmental public body established under section 10 of the Health and Safety at Work etc. Act 1974 (HSWA), as amended. We are also listed as a Competent Authority under Section 28(7) of DPA 2018.

HSE processes special category data and criminal offence data under the following DPA 2018, Schedule 1 conditions;

Reference	Title
Part 1(1)	**Employment, Social Security and Social Protection**
HSE may process data concerning racial or ethnic origin, religious or philosophical beliefs, trade union membership, sexual orientation, health and criminal offence data for the purposes of performing its obligations or rights as an employer, or for ensuring the social protection of individuals.	
Part 2(6)	**Statutory etc. and government purposes**
HSE may process data concerning health, trade union membership, and criminal offence data for the purpose of exercising its statutory obligations under HSWA 1974.	
Part 2(8)	**Equality of Opportunity**
HSE may process data concerning racial or ethnic origin, religious or philosophical beliefs, sexual orientation and health for the purposes of monitoring equality of opportunity or treatment between groups of its employees with a view to enabling such equality to be promoted or maintained.	
Part 2(9)	**Racial and ethnic diversity at senior levels in HSE**
HSE may process data concerning racial or ethnic origin for the purposes of promoting and maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in our organisation.	
Part 2(10)	**Preventing or detecting unlawful acts**
HSE may process data concerning health and criminal offences for the purposes of preventing and detecting crimes.	
Part 2(11)	***Protecting the public against dishonesty etc.***
HSE may process data concerning criminal convictions for the purpose of protecting the public from serious harm caused by dishonest or non-compliant working practices.	
Part 2(12)	**Regulatory requirements relating to unlawful acts and dishonesty**
HSE may process data concerning health and criminal offences for the purposes of its core regulatory functions as defined under HSWA 1974. This includes (but not limited to) investigations into workplace health and safety incidents or instances of occupational ill health, and for the prosecution of serious criminal breaches of health and safety law.	
Part 2(13)	***Journalism etc. in connection with unlawful acts and dishonesty etc.***
HSE may publish personal data concerning criminal offences associated with the commission of unlawful acts by a person or dishonesty, malpractice or other seriously improper conduct by a person where HSE believes that publication is in the public interest	

HSE does not process genetic data, or biometric data for the sole purpose of identifying a natural person. Furthermore, HSE does not process personal data concerning political opinion.

Compliance with Data Protection Principles

In accordance with the accountability principle, HSE maintains records of processing activities under Article 30 of the UK GDPR and section 61 of the DPA 2018. We carry out data protection impact assessments where appropriate in accordance with Articles 35 and 36 of the UK GDPR and section 64 of the DPA 2018 to ensure data protection by design and by default.

In accordance with UK GDPR Article 37 and based on its status as a UK public authority, HSE has appointed a permanent Data Protection Officer (DPO).

In addition, we have effective breach notification systems and procedures in place that ensure timely reporting to the ICO (where necessary) and appropriate actions are taken to limit the impact of the breach on the affected data subjects.

HSE follows the data protection principles set out in Article 5 of the UK GDPR, and Part 3, Chapter 2 of the DPA 2018 for law enforcement processing, as follows.

Lawfulness, Fairness and Transparency

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

HSE will;

- ensure that personal data is only processed where it is lawful to do so
- ensure a lawful basis for processing personal data is identified against each business function, and set out within our Records of Processing Activities
- ensure that data subjects are appropriately informed of all processing activities performed by HSE on their personal data (excluding certain areas of law enforcement processing). This will be achieved through the use of a tiered privacy notice published on our website, and just in time notifications where appropriate.

Purpose Limitation

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

HSE will;

- only collect personal data for specified, explicit and legitimate purposes,
- inform data subjects of those purposes via the published privacy notice and other notification mechanisms
- not use personal data for purposes that are incompatible with the purposes for
  which it was collected.
- Inform the data subject before using personal data for a new purpose that is not
  compatible with the original purpose.

Data Minimisation

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

HSE will;

- only process the minimum personal data needed for the purpose for which it is collected
- ensure that the data we collect is adequate and relevant
- ensure the least intrusive personal data processing method is adopted in each instance
- Periodically review data held and delete anything no longer required

Accuracy

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

HSE will;

- Ensure appropriate processes are in place to check the accuracy of the data we create and collect, and to maintain that accuracy for the duration of the processing
- Ensure the sources of the personal data we create and collect are reliable
- Ensure the individual's right to rectification is observed and applied in a timely manner

Storage Limitation

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.

HSE will;

- be aware of the personal data held and why it is needed
- give due consideration and justification for the retention of personal data

- ensure personal data is destroyed in accordance with HSE's business classification scheme and disposal policy
- regularly review and erase or anonymise personal data no longer required
- ensure processes are in place that observe and enforce the data subjects' right to erasure

Integrity and Confidentiality

Personal data shall be processed in a manner that ensures appropriate security of
the personal data, including protection against unauthorised or unlawful processing
and against accidental loss, destruction or damage, using appropriate technical or
organisational measures.

HSE will;

- ensure that there appropriate organisational and technical measures in place
  to protect personal data
- maintain Cyber Essentials security accreditation at all times
- provide annual data protection training to all staff
- employ technical security controls to secure sensitive information within systems
- implement role-based access controls to restrict access to sensitive data

Policy Review

This policy instrument will be kept under review and, as a minimum, will be subject to formal evaluation on an annual basis.