



## Data Protection (Employment) Policy

Version	5
Date Approved	22 June 2018
Date of Previous Approval	15 May 2018 31 March 2017 8 December 2015 12 December 2013 27 February 2013
Date of Next Review	May 2020

You may also be interested in the following policies:

[Clear Desk Policy](#)  
[Removable Media Policy](#)

## 1. Purpose

- 1.1. The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC.
- 1.2. The GDPR places responsibilities on any organisation to process personal data that it holds in a fair and proper way. This is the Commission's policy and statement on the purposes for which it holds personal data about its employees and others who work for it.
- 1.3. Under the GDPR, the data protection principles set out the main responsibilities for organisations.
- 1.4. Article 5 of the GDPR requires that personal data shall be;
  - a) processed lawfully, fairly and in a transparent manner in relation to individuals;
  - b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
  - c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
  - d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
  - e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
  - f) 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."
- 1.5. Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

## 2. Rights for Individuals

- 2.1. The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

2.2. Definitions of these rights are available on the Information Commissioners Office website at; <https://ico.org.uk/for-the-public/>

2.3. We will inform you about the collection and use of your personal data. We will provide you, as required, with information including: our purposes for processing your personal data, our retention periods for that personal data, and who it will be shared with. We call this 'privacy information'. We will advise you of this privacy information at the time we collect your personal data.

2.4. We will regularly review, and where necessary, update our privacy information. We will advise you of any new uses of your personal data to their attention before we start processing it.

### 3. Sensitive Personal Data

3.1. The GDPR refers to sensitive personal data as "special categories of personal data". Definitions of these special categories are below;

3.2. Article 9 of the GDPR states;

**“Processing of special categories of personal data**

1.Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.”

3.3. Article 10 of the GDPR states;

**“Processing of personal data relating to criminal convictions and offences**

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.”

3.4. We will collect, hold and process information consisting of personal data including sensitive personal data about all our employees, applicants for employment, agency workers and others who work for us, and who are referred to in the GDPR as “data subjects”.

3.5. The purpose for which we hold information about data subjects is for administrative and personnel management and legal requirements including, but not limited to;

- Recruitment
- Appraisals
- Performance
- Promotion
- Training
- Career Development
- Pay And Remuneration
- Pension And Insurances And Other Benefits
- Payroll
- Tax,
- National Insurance
- Other Deductions From Pay
- Health And Safety
- Disciplinary
- Grievances
- Review Of Our Human Resources Policies
- Monitoring Purposes.

## **4. Statutory Purposes**

4.1. In addition, we may collect, hold and process data including sensitive personal data, if it is necessary to do so, for compliance with any statutory duty with which we are required to comply. This will be undertaken in adherence with the GDPR.

## **5. Employee Obligations**

5.1. In connection with their own personal data all staff should

- (i) Ensure that any information that they provide to the Commission in connection with their employment is accurate and up to date.
- (ii) Inform the Commission of any change for which they are responsible, for example changes of address, telephone number etc.

5.2. In addition all employees must ensure that they understand their own responsibilities with regards to Data Protection and the GDPR within their own area of work. Employees should;

- (i) Ensure that any personal data which they process is kept securely and as per the Commission's systems and processes.
- (ii) Ensure that personal information is not disclosed either orally or in writing, intentionally or otherwise to any unauthorised third party
- (iii) Ensure they follow the Commission's Clear Desk Policy (Appendix 1) to ensure the security of all relevant data and information.

- 5.3. Unauthorised disclosure may be a disciplinary matter and could be considered gross misconduct in certain cases. Employees should make reasonable efforts to ensure that all personal information is kept securely and should pay particular attention to the security of sensitive data.
- 5.4. All personal data should be accessible only by those who need to use it and sensitive data must be kept only in a lockable room with controlled access or kept in a locked filing cabinet or drawer, if computerised, be password protected or kept only on discs which are themselves kept securely.
- 5.5. Employees need to take appropriate security precautions in respect of day to day laptop/PC usage. Care must be taken to ensure that laptops/PCs and terminals are not visible except to authorised employees and that computer passwords are kept confidential. Screens should not be left unattended when personal data is being processed and manual records should not be left where they can be accessed by unauthorised staff. When manual records are no longer required, they should be shredded and disposed of securely.

## **6. Data Protection Officer**

- 6.1. The GDPR introduces a duty for the Commission to appoint a data protection officer (DPO).
- 6.2. The Commission's DPOs will assist the organisation to monitor internal compliance, inform and advise on y data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.
- 6.3. In appointing a DPO the Commission will ensure the following;
  - The DPO reports directly to the highest level of management and is given the required independence to perform their tasks.
  - The DPO, in a timely manner, is involved in all issues relating to the protection of personal data
  - The DPO is sufficiently well resourced to be able to perform their tasks.
  - The DPO will, not be penalised for performing their duties.
  - The Commission will take account of our DPO's advice and the information they provide on our data protection obligations.
  - Any other tasks or duties assigned to the DPO will not result in a conflict of interests with their role as a DPO.

### **Tasks of the DPO**

- 6.4. The DPO is tasked with monitoring compliance with the GDPR and other data protection laws, data protection policies, awareness-raising, training, and audits.
- 6.5. When carrying out a DPIA, the advice of the DPO will be sought, and the DPO will monitor the process.
- 6.6. The DPO will act as a contact point for the ICO. They co-operate with the ICO, including during prior consultations under Article 36, and will consult on any other matter.

6.7. When performing their tasks, the DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

**Accessibility of the DPO**

6.8. The DPO is easily accessible as a point of contact for our employees, individuals and the ICO.

6.9. We have published the contact details of the DPO and communicated them to the ICO.

**7. Variation**

7.1. The Commission reserves the right to vary this Policy as it deems appropriate to include compliance with any legal requirements.