Ethical Standards Commissioner

**Commissioner for Ethical Standards in Public Life in Scotland**
Thistle House
91 Haymarket Terrace
Edinburgh
EH12 5HE

# DATA PROTECTION POLICY

Date policy adopted: 01/04/2011
Date of last review: 27/10/2021

The contents of this policy have been developed with reference to the Data Protection Act 2018 and guidance available on the Information Commissioner's website, in particular the *Guide to the UK General Data Protection Regulation* available during August 2021.

## 1. Purpose and Scope

The UK General Data Protection Regulation and the Data Protection Act 2018 ('the GDPR') stipulate how personal data should be managed and give individuals certain rights regarding the information held about them.

In order to carry out its statutory functions, the Commissioner for Ethical Standards in Public Life in Scotland ('ESC') processes personal data. This document outlines ESC policy in relation to the GDPR. ESC has separate policies relating to the requirements of the Freedom of Information (Scotland) Act 2002 and the Public Records (Scotland) Act 2011.

This policy applies to all employees and to contractors with access to personal data.

The GDPR requires ESC to appoint a Data Protection Officer ('DPO') to inform and advise on our data protection obligations. The DPO service is provided through the Scottish Parliamentary Corporate Body.

The Information Commissioner's Office ('ICO') is responsible for upholding information rights in relation to personal data across the UK.

## 2. Policy Statement

ESC is committed to ensuring that personal data is managed safely, effectively and in line with the requirements of the GDPR.

## 3. Implementation, monitoring and review of the policy

Overall responsibility for policy implementation, monitoring and review lies with ESC. Everyone covered by the scope of the policy is obliged to adhere to, and facilitate implementation of the policy. Appropriate action will be taken to inform all new and existing employees and others covered by the scope of the existence of the policy and their role in adhering to it.

Following the UK's departure from the European Union, the UK continues to follow the basic principles of the EU GDPR as laid down in the Data Protection Act 2018 but has the independence to change this legislation in future. From June 2021 the EU has adopted an adequacy decision which enables personal data to freely flow between the EEA and UK and vice versa.

The policy will be reviewed at such times as changes to UK legislation, the adequacy decision or ESC's policy position requires it. The policy will be made available to the general public.

## 4. Data protection principles

4.1 The GDPR requires that personal data be:

a. processed fairly, lawfully and transparently
b. collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes
c. adequate, relevant and limited to what is necessary
d. accurate and, where necessary, kept up to date, Inaccurate data should be erased or rectified without delay.
e. not be kept for longer than necessary
f. held securely and appropriate measures shall be taken against unauthorised or unlawful processing and against its accidental loss, damage or destruction.

4.2 ESC is responsible for and must be able to demonstrate compliance with the principles.

## 5. Personal data

5.1 Personal data means any information relating to an identified or identifiable living individual (the 'data subject').

5.2 'Identifiable living individual' means a living individual who can be identified, directly or indirectly from the information held, in particular by reference to:

a. an identifier such as a name, an identification number, location data or an online identifier (e.g. an IP address), or
b. one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

5.3 Personal data can include addresses, telephone numbers, photographs, video and audio recordings and other personal details. It also includes any expression of opinion about a living individual or any indication of intentions about that individual.

5.4 The GDPR applies to personal data held both electronically and in paper filing systems.

5.5 Personal data that has been anonymised does not fall within the scope of the GDPR.

5.6 Personal data that has been pseudonymised can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

## 6. Processing personal data

6.1 Processing means any operation performed on personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

6.2 The GDPR applies to 'controllers' **and** 'processors'.
a. A controller determines the purposes and means of processing personal data. ESC is a data controller.
b. A processor is responsible for processing personal data on behalf of a controller. ESC uses a limited number of third parties (processors) to process data on ESC's behalf (the data controller). Examples include payroll processing services, the Civil Service Pension Scheme, and Public Appointment Advisers.

6.3 ESC is registered with the ICO as a data controller. Details of the ESC registration can be found on the ICO's website – https://ico.org.uk/esdwebpages/search.

## 7. Special categories of personal data

7.1 The GDPR recognises the following as special categories of personal data.
a. Data revealing:
   i. Racial or ethnic origins
   ii. Political opinions
   iii. Religious or philosophical beliefs
   iv. Membership of a trade union
b. Genetic data
c. Biometric data for the purpose of uniquely identifying a person
d. Data concerning health
e. Data concerning an individual's sex life or sexual orientation

7.2 Processing special category data is prohibited unless in one or more of the following specific circumstances.
a. The data subject has given explicit consent
b. It is necessary to meet statutory obligations in relation to employment legislation
c. To protect the vital interests of an individual where they are physically or legally incapable of giving consent
d. Processing carried out in relation to its legitimate activities by a foundation, association or not-for-profit body with a political, philosophical, religious or trade union aim and solely relates to the personal data of members, former members and those who have regular contact with the body. Data should not be disclosed outside the body without the consent of the data subjects.
e. The personal data are manifestly made public by the data subject
f. For the establishment, exercise or defence of legal claims
g. For the purpose of substantial public interest
h. For the purposes of preventative or occupational medicine
i. For reasons of public interest in the area of public health
j. For archiving purposes in the public interest

## 8. Criminal convictions and offences

8.1 A lawful basis and either legal authority or official authority is required to process personal data about criminal convictions or offences.

8.2 Further guidance should be sought from the ICO when processing this form of information.

## 9. Lawful basis

9.1 The first principle of the GDPR requires that ESC processes all personal data lawfully, fairly and in a transparent manner. There are six lawful ways to process personal data.

9.2 Public task: the processing is necessary for a) carrying out a specific task in the public interest or b) in exercising official tasks, functions, duties or powers, and the task has a clear basis in law. This is the most common basis for ESC to process personal data.

9.3 Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).

9.4 Contract: the processing is necessary for fulfilling a contract with an individual, or because the individual has asked for specific steps to be taken before entering into a contract.

9.5 Consent: the individual has given clear consent to process their personal data for a specific purpose. ESC can only rely on this in limited circumstances.

9.6 Legitimate interests: the processing is necessary for ESC to achieve a legitimate interest and is balanced against the individual's interests, rights and freedoms. ESC can only rely on this in limited circumstances.

9.7 Vital interests: the processing is necessary to protect someone's life.

## 10. Rights of the individual

10.1 The GDPR gives individuals certain rights.

10.2 Requests made under these rights are known as information requests.

10.3 The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. Individuals must be informed of this right at the time their personal data is collected and as early in the process as possible. ESC achieves this through reference to and publication of Privacy Notices, which are available on the ESC website and linked in all email footers. More specific information on the collection and retention of personal data is provided at the point data is collected wherever possible, such as on the ESC Complaint Form and in application packs for external recruitment.

10.4 The right of access

Under the GDPR, individuals have the right to obtain confirmation that their data is being processed, access to their personal data and other supplementary information (normally available through the Privacy Notice). When the individual asks for this, it is called a subject access request.

10.5 The right to rectification
The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.

10.6 The right to erasure
The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. The right is not absolute and only applies in certain circumstances. For instance, the right is superseded where ESC needs to process or retain personal data in order to fulfil statutory obligations.

10.7 The right to restrict processing
Individuals have the right to request the restriction or suppression of their personal data. This is an alternative to requesting the erasure of their data.

10.8 The right to data portability
The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller. This right primarily applies to banks or other commercial organisations that might need to transfer data at a customer's request, and is unlikely to apply to ESC.

10.9 The right to object
The GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask for the processing of their personal data to stop.

10.10 Rights in relation to automated decision making and profiling
The GDPR restricts the making of solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals. ESC does not currently process personal data in this way.

10.11 Detailed procedures for responding to information requests are available in a separate document 'Data Protection Procedures'.

## 11. Accountability

11.1 The GDPR introduces a new data protection principle that says organisations are responsible for, and must be able to demonstrate, compliance with the other principles. This requires ESC to ensure evidence is retained in the form of an audit trail for all data protection decisions, breaches, policy and procedures.

## 12. The role of the ICO

12.1 The ICO is responsible for enforcing and promoting the UK's data protection laws. The ICO:
a. investigates complaints brought to them and issues legally enforceable decisions
b. promotes good practice and offers advice to individuals and organisations
c. maintains a register of data controllers
d. investigates data breaches.

12.2 The ICO has a number of powers to enforce the GDPR and can issue penalties of up to £17,500,000 or 4% of turnover.

## 13. Our roles and responsibilities

13.1 Ultimate responsibility for compliance with the GDPR lies with the Commissioner.

13.2 In order that ESC can meet this responsibility, all employees and contractors with access to personal data must be able to:

a. consider the implications of data protection to their role
b. recognise personal data
c. keep all personal data securely
d. only disclose personal data for authorised purposes
e. keep all personal data accurate and up to date
f. dispose of personal data safely and in accordance with the Retention Schedule.
g. identify an information request
h. forward information requests to those employees trained to respond
i. familiarise themselves with and follow ESC data protection policy and procedures

13.3 The Head of Corporate Services acts as the ESC information officer and is responsible for:

a. recording all information requests received
b. monitoring whether responses are issued within the terms of the GDPR
c. providing advice to the Commissioner and other employees about the GDPR and on how to respond to information requests
d. providing the Senior Management Team with statistics on information requests and reviews, highlighting any key issues and trends and flagging any lessons to be learned
e. maintaining their knowledge of GDPR and data protection best practice
f. maintaining this policy and other guidance
g. assisting the DPO in their duties, including the reporting of personal data breaches.

13.4 The Business Officer assists the Head of Corporate Services with these duties and provides cover for annual leave, etc.

13.5 Data protection matters will be reviewed at meetings of the Senior Management Team.

13.6 Line managers will identify whether the employees for whom they are responsible have sufficient knowledge of data protection and ESC procedures. Knowledge in this area will be examined during the employee's annual appraisal and any specific training requirements identified. Issues arising during the year will be referred to the Head of Corporate Services who will arrange ad hoc training as necessary

13.7 Employees concerned about handling personal data should contact their line manager without delay.

13.8 Any misuse of personal data by employees will be treated extremely seriously and may constitute a disciplinary offence under the disciplinary policy.

## 14. Training arrangements

14.1 ESC will:

a. provide training to ensure that all employees have sufficient knowledge of the data protection
b. ensure that employees with responsibility for responding to information requests have undertaken appropriate training to ensure that responses meet statutory requirements
c. provide appropriate training for employees responsible for providing advice and guidance
d. ensure that training is refreshed on a regular basis

14.2 Arrangements will be flexible, allowing for ad-hoc training when necessary.

## 15. Identifying information requests

15.1 ESC must respond to information requests within one month. Therefore, it is important that all information requests are identified promptly.

15.2 Postal requests or those sent to general inboxes will be captured by relevant employees in the Corporate Services Team.

15.3 Employees should be aware that they may receive information requests directly to their own mailbox. These still constitute valid requests and must be answered within one month of the email arriving in the inbox.

15.4 Employees should arrange for a colleague to check their email inbox if they are absent for any length of time in case any requests have been sent directly to them. This should be done even where an out of office alert has been activated – a request is still considered as received by the authority even if an out of office alert has been sent back to the requester.

15.5 A subject access request may not be explicitly identified as such by the requestor, so all employees must be alert for any requests for information. Examples would include a respondent asking for a copy of their own case file or report, or a witness requesting the case report.

15.6 Employees should also be aware that requests for information may also fall under Freedom of Information legislation as well as data protection.

A separate Data Protection Procedures document outlines specific actions to be undertaken when implementing key elements of the above policy. These procedures will normally be undertaken by the Corporate Services Team or the DPO.

**Equality Impact Assessment**

Does this policy comply with the general Public Sector Equality Duty (s149 Equality Act 2010)?

This policy applies to all employees. Its impact was considered when drafting. We consulted with all employees prior to publication to identify and address any issues.

Ethical Standards Commissioner

## Data Protection Impact Assessment

Have we considered any effect the policy may have on the collecting, processing and storing of personal data?

This policy is a policy statement document relating to data protection and will not generate any records.

## Information Security Impact Assessment

Have we considered the impact any policy may have on our cyber-resilience?

This policy should have no impact on our cyber-resilience.

## Records Management Impact

Have we considered the impact any policy may have on our ability to manage our records?

This policy should help improve our ability to manage our records.

| Version | Description | Date | Author |
|---|---|---|---|
| 1.0 | First draft | 24/08/2021 | Corporate Services |
| 1.1 | Update to phone number | 16/05/2023 | Corporate Services Officer |