EQUALITY COMMISSION FOR NORTHERN IRELAND

Data Protection Policy
and
Procedural Guidance

Introduction

This document sets out the Equality Commission's approach to the protection of personal data. It is designed to ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work, and their rights and responsibilities in respect of the personal information held by the Commission.

Policy Statement

The Commission is fully committed to protecting the rights and privacy of individuals in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (the 2018 Act).

The Commission is required to retain and process personal information about its staff, Commissioners, service-users and other individuals it has dealings with for a range of activities. These include administrative functions, personnel, research, advice, statutory obligations, advising and supporting individual litigants, and other business related activities.

To comply with the law, there must be a lawful basis[1] for processing personal information and it must be collected and used fairly, stored safely and securely, and not be disclosed to any third party unlawfully.

[1] Lawful basis includes Consent of the individual, a Contract with the individual, Compliance with a Legal Obligation, Vital Interests, or fulfilment of a Public Task, and Legitimate Interests.

Any breach of the GDPR or the 2018 Act is considered to be an offence and in that event, the Commission's disciplinary procedures may apply.

As a matter of good practice, other agencies and individuals working with the Commission who have access to personal information, including barristers, solicitors and other third parties acting for the Commission, will be expected to have read and to comply with this policy.

Scope

The policy applies to all Commission staff[2] and Commissioners, who must be familiar with this policy and comply with it at all times.

The policy relates to all personal data[3], including sensitive personal data[4] held by the Commission whether in computerised records or in filing systems and other manual media.

This policy complements the Commissions other policies relating to internet and email use. The Commission may supplement or amend this policy by additional policies and guidelines from time to time.

Commission Responsibilities

The Commission as a body corporate is the data controller[5] under the Act.

Compliance with data protection legislation is the responsibility of all individuals who process personal information.

---

[2] Including all employees, agency staff or any other person contracted by the Commission.
[3] meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
[4] The GDPR refers to sensitive personal data as "special categories of personal data" which specifically include genetic data, and biometric data where processed to uniquely identify an individual.
[5] Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Staff of the Commission are responsible for ensuring that any personal data supplied by them to the Commission is accurate and up-to-date.

A Data Protection Officer has been appointed who is responsible for overseeing the operation of data protection across the Commission. However, Divisional managers and other staff also have important roles and hold personal responsibility for the data they have access to.

Details of the Commission's registration with the Information Commissioner are published on the Information Commissioner's website. Anyone who is, or intends, processing data for purposes not included in the Commission's Registration should seek advice from the Data Protection Officer.

The Commission's **Data Protection Officer** is:

Eoin O' Neill
Solicitor to the Commission
Tel. 028 90 890859
Email eoneill@equalityni.org

The Commission also has in place an] **Information Asset Security Manager (IASM)**, who has operational responsibility for the Commission's data protection and information security arrangements.

The Commission's IASM is Gary Rafferty, Manager ICT.

The Data Protection Officer will;

- Ensure that the Commission is properly registered under the Act; with the Information Commissioners Office.

- Provide advice on interpreting the GDPR and the 2018 Act and the 'data protection principles' contained within it;

- Provide guidance to staff about their individual responsibilities and the procedures they should follow;

- Keep Commissioners updated about data protection responsibilities, risks and issues;

- Ensure the review of data protection procedures and policies on a regular basis;

- Arrange data protection training and advice for staff, Commissioners and those covered by this policy;

- Answer questions on data protection from staff, board members and other stakeholders;

- Respond to queries and deal with subject access requests in line with the agreed procedure;

- Check and approve third party contracts or agreements regarding data processing.

Employee responsibilities

Under their Terms and Conditions of Employment, Commission staff are advised that information about them may be included in computer files and manual records held by the Commission. A copy of this document is provided at induction.

Staff must take reasonable steps to ensure that personal data the Commission holds about them is accurate and updated as required. For example, if their personal circumstances change, staff should inform the Data Protection Officer or the HR team so that their records can be updated.

If, as part of their responsibilities, employees collect information about other people, they must comply with GDPR and the 2018 Act, this Policy and Procedure and with any other data protection guidance provided by the Data Protection Officer, line manager or other senior member of staff. They should comply with the policies and guidelines in the Information Security section on the intranet.

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed orally, in writing or otherwise to any unauthorised third party.

Staff are required to use information technology and communication facilities sensibly, professionally and lawfully and in line with the Commission's ICT policies and procedures. Particular care should be taken when using e-mail and the intranet.

Employees are legally responsible for the records they hold, create or use in the course of their employment, including client, corporate and administrative records whether paper-based or electronic, including e-mails. All such records may be subject to GDPR and the 2018 Act, as well as available to the general public, with limited exceptions, under the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

Employees are required to follow the Commission's Record Management Policy and related guidance. Any member of staff, or other data subject, who considers this policy has been breached, should raise the matter with the Commission's Data Protection Officer, in the first instance.

Rights of individuals

The Commission will ensure that the rights of individuals, including staff, about whom personal data is held can be fully exercised.

Individuals on whom the Commission holds personal data have the following rights in respect of that data;

- to be informed;
- of access;
- to rectification;
- to erasure (the right to be forgotten);
- to restrict processing;
- to data portability;
- to object;

Employees and other subjects of personal data held by the Commission have the right to be informed of and to access any personal data that is being kept about them on computer and also have access to paper-based data held in certain manual filing systems. This right is subject to certain exemptions which are set out in the 2018 Act.

Any person who wishes to exercise this right should make the request in writing to the Commission's Data Protection Officer, following the '**Procedure for Subject Access Requests & Other Individual Rights**'.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection breaches.

This allows the Commission to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Information Commissioners Office (ICO), where necessary, of any compliance failures that are material either in their own right or as part of a pattern of failures

Consequences of failing to comply

The Commission takes compliance with this policy very seriously. Failure to comply puts the staff member responsible and the organisation at risk.

Failure to comply with the Commissions requirement s may lead to disciplinary action under its procedures which could result in dismissal.

Training

All staff will receive training on this policy. New recruits will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or in this policy and procedure.

Training will cover both:

- The law relating to data protection; and
- Our data protection and related policies and procedures.

Monitoring

The DPO has overall responsibility for this policy. He will make a quarterly report to the Senior Management Team relating to compliance with this policy, detailing any actual or potential breaches and any requests relating to the exercise of individual rights.

Review

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the 2018 Act. In any event, it will be reviewed, at least, every 3 years.

Procedural Guidance

Guiding Principles

The Commission will process personal data in compliance with the data protection principles:

1. Fair and lawful processing:

The Commission will process personal data fairly and lawfully in accordance with individuals' rights. The Commission will ensure that any use of personal data is justified using at least one of the lawful conditions for processing and this will be specifically documented. This means that it will not process personal data unless the individual whose details we are processing has actively consented to this happening, or there is an alternative lawful basis. All staff who are responsible for processing personal data must be aware of the conditions for processing. The conditions for processing being relied upon will be available to data subjects in the form of a privacy notice.

Where the Commission processes sensitive personal data the data subject's *explicit* consent to do this will be sought unless exceptional circumstances apply or we are legally required to process it. Any such consent will clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

2. Specified, explicit and legitimate purposes

Any personal information held by the Commission will have been collected for specified, explicit and legitimate purposes, and will not be further processed in a manner that is incompatible with those purposes.

The Commission's Privacy Notices set out the purposes for which personal data is held. They also explain that the Commission may be required to give information to third parties such as auditors, expert witnesses and other professional advisers and to enforcement agencies for the detection and prevention of crime.

The Notices emphasise that data subjects have a right of access to the personal data that is held about them.

3. Adequacy and Relevance of Data

Any personal information held by the Commission will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

4. Accuracy of Data

The Commission will ensure that any personal data it processes is accurate and up-to-date, and not excessive, given the purpose for which it was obtained. It will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Every reasonable step will 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.

Individuals may ask that we correct inaccurate personal data relating to them is corrected.

5. Data Retention

The Commission will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, and in a manner consistent with the Commission's data retention and disposal schedules.

6. Data Security

Personal data will be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. In particular;

- In cases when data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it.

- Printed data will be shredded when it is no longer needed

- Data stored on a computer should be protected by strong passwords that are changed regularly. All staff should use a password manager to create and store their passwords.

- Data stored on CDs or memory sticks, or in written format, must be locked away securely when not in use.

- The DPO must approve any cloud used to store data.

- Servers containing personal data must be kept in a secure location, away from general office space.

- Data should be regularly backed up in line with the company's backup procedures.

- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.

- All servers containing sensitive data must be approved and protected by security software and a strong firewall.

- All staff must comply with the full range of policies and guidelines detailed under Information Security, Policy Documents on the Commission's Intranet.

Data Protection Audit and Register

The purpose for holding personal data and a general description of the categories of people and organisations to whom the Commission may disclose it are listed in our Data Protection register. This information may be inspected or obtained from the Information Commissioner's Office and can also be found on the Commission's intranet and website.

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

Transparency (Privacy Notices)

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. This information is set out in Privacy notices.