Protection of Personal Data

Code of Practice

September 2018

"Everyone has the right to the protection of personal data concerning him or her."

(Charter of Fundamental Rights of the European Union)

Data Protection Principles

1 **Transparency**

2 **Purpose limitation**

3 **Data minimisation**

4 **Accuracy**

5 **Retention and storage**

6 **Security and confidentiality**

Table of Contents

Introduction

The General Data Protection Regulation and the Data Protection Act 2018 (the 2018 Act) introduced enhanced rights for data subjects in relation to the protection of their information and personal data. The security and protection of personal information that we collect and hold is of critical importance to us and the bodies we audit. It is vitally important that we maintain the highest standards in safeguarding confidential data and the confidence of the public.

Information is the foundation of the conduct of our business as our work is based on routines involving the examination of documentation, enquiries from administrators, inspections and third party confirmations. A primary source of evidence is the records of the audited body. These records and the related documentation are personal information to the extent that they relate to living individuals. We have been given a statutory right of access to data and information to ensure that we are effective in the discharge of our statutory functions.

All of us are expected to treat personal information with the greatest possible care and to ensure that it will be accessed only when necessary for our audit and examination purposes. It is up to each member of staff to take personal responsibility for ensuring that data is not accessed or disclosed inappropriately.

Our obligations in relation to safeguarding data are reinforced by a range of legislative and administrative provisions that are designed to protect the rights and interests of citizens and businesses. These provisions include the Official Secrets Act 1963, the General Data Protection Regulation, Irish data protection legislation, the professional ethical standards and the Civil Service Code of Standards and Behaviour, which create obligations in relation to the confidentiality of official data and the protection of records against unauthorised access, unnecessary use, alteration, destruction or disclosure.

This Code represents best practice of protecting information held by the Office of the Comptroller and Auditor General.

Colette Drinan
Secretary and Director of Audit

Data Protection Code of Practice

Purpose

Set against the General Data Protection Regulation and Irish data protection legislation the aim of this Code of Practice is to ensure each employee of the Office of the Comptroller and Auditor General (the Office) has an understanding of the concepts of Data Protection and is aware of their own responsibilities. This will assist the Office in its compliance with the Irish data protection legislation. This Code applies to all records generated or obtained by the Office, which contain personal information relating to individuals.

Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. Under the General Data Protection Regulation and Irish data protection legislation, certain categories of data must be registered with the Data Protection Commission.

The general public and audited bodies are entitled to know that their information is being processed for legitimate purposes and disclosed only where permissible by law.

There are six key principles set out in Article 5 of the General Data Protection Regulation.

- transparency
- purpose limitation
- data minimisation
- accuracy
- retention and storage
- security and confidentiality.

The Code of Practice sets out how we apply these principles and what is expected of our staff. The Code also sets out the accountability arrangements for data protection within the Office.

Principle 1 – transparency

Data processing is undertaken in a transparent manner and data subjects are provided with certain information in relation to processing of their personal data.

We collect, hold and process data in accordance with our statutory functions of audit, examination and inspection, or in relation to the administrative operations of the Office.

An audit involves accessing and testing a variety of information, for example payments by audited bodies to individuals. Audit staff have the authority to request information and explanations necessary for the purpose of our work. Section 10 of the Comptroller and Auditor General (Amendment) Act 1993 gives us the statutory authority for collecting data and Section 38 of the Data Protection Act 2018 gives us the authority to process this information.

We are committed to treating the information given to us in confidence and ensure that it will not be used or disclosed except as provided for by law. Requests will be requisitioned in accordance with an audit plan or scope of an examination and approach authorised by a manager.

Under the General Data Protection Regulation, a data subject has a right to

- Information (e.g. the purpose(s) for processing his/her data;
- Access information (e.g. data being kept about him/her)
- Rectification of personal data
- Erasure (right to be forgotten)
- Restriction of processing
- Data portability and to object to processing
- Not be subject to automated individual decision making.

Section 60 of the 2018 Act provides for a restriction on the exercise of these rights in relation to the exercise of our statutory functions.

Principle 2 - purpose limitation

Personal data is only processed for the particular purpose(s) for which it was collected (and for closely related purpose(s)).

International auditing standards require us to obtain and keep evidence including working papers, to support our opinions on financial statements and to support findings and conclusions in the reports on examinations of value for money.

We only use personal information for the purposes for which it was given to us, or for purposes which are directly related to our statutory functions. We do not give it to other government departments, bodies or anyone else unless one of the following applies:

- the individual has consented;
- the individual would reasonably expect, or has been told, that information of that kind is usually passed to those individuals, departments or bodies;
- it is otherwise required or authorised by law; or
- it is reasonably necessary for the enforcement of the criminal law or for the protection of public revenue.

For the purposes of the General Data Protection Regulation and Irish data protection legislation, processing of personal data by contractors on behalf of the Office does not constitute disclosure. However, such transfers must be subject to appropriate contractual agreements including provisions relating to data protection with specific security and disposal/retention arrangements. Our staff are instructed through operating procedures in relation to transfers of data and responsibilities of contractors when handling our data.

Principle 3 - data minimisation

The collection of personal data is limited to what is adequate, necessary and relevant to the purposes for which it was collected.

International auditing standards set out the procedures to be adopted by auditors in obtaining sufficient and appropriate evidence for the purpose of their work. We issue guidance to staff and provide training in order to comply with auditing standards and this data protection principle. The guidance emphasises the need for staff to ensure that information requested is the minimum necessary to achieve the audit or examination testing objective.

Where large or entire datasets including personal information are requested for sampling or analysis

- the requests will be authorised by a Deputy Director
- the data will be held on the audited body's or Office's ICT network
- the data set will be anonymised by the audited body where possible.

Principle 4 - accuracy

Personal data must be accurate and kept up-to-date and every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified.

We collect and process personal information for administrative purposes including information on current and former employees, suppliers and others with whom we communicate. Staff also have access to their personal data held on shared service systems which they can update to ensure their accuracy.

The Deputy Director, Corporate Services, has been assigned responsibility as the Data Controller and the Security Officer has been assigned the role of Data Protection Officer.

In order to comply with this principle staff should ensure that:

- the general requirement to keep personal data up-to-date has been fully implemented;
- manual and computer procedures are adequate to ensure high levels of data accuracy;
- appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up-to-date;
- procedures are in place to ensure personal data held is accurate, including reviewing records on a regular basis, identifying areas where errors are most commonly made and providing training, etc.
- every individual has a right to have inaccurate information rectified or erased. Support staff will explain how they can interact and assist colleagues (and others) to ensure data accuracy.

Principle 5 - retention and storage

Personal data is not to be kept for any longer than the purposes for which it was collected or required by law or other circumstances.

We have a Records Retention and Disposal Policy which sets out how long different classes of records will be held.

In general, the retention period for data within the Office is subject to legislative provisions pertaining to the area involved or for business requirements. For example, personnel data would be retained only for as long as permitted by employer/employee legislation, amongst others.

In the case of audit records, international auditing standards require that we have evidence to support our opinions and reports. This necessitates the retention of data for a reasonable period of time after the completion of an audit and examination. Records relating to audits and examinations are generally retained for a period of seven years after the C&AG has reported on the matter. This can be extended in certain circumstances.

We are legally obliged to seek authorisation from the Director of the National Archives in relation to the destruction of all records that are subject to that legislation. We delete records relating to audits and examinations, in accordance with the legislation and our Records Retention and Disposal Policy. The capture and retention of CCTV footage is included in this policy.

Principle 6 - security and confidentiality

Technical and organisational security measures be put in place to ensure that personal data is protected from various forms of data breaches.

High standards of physical and technical security are essential to protect the confidentiality of personal data. We expect the highest standards of information and data security from all our staff. To that end we have appropriate security measures in place which include, inter alia,

- maintaining ISO 27001 Information Security Management certification
- ensuring access to information is restricted to authorised staff and extends only to that information necessary to carry out their appointed duties
- keeping premises secure, especially when unoccupied
- ensuring computer systems are physically secure and access is controlled
- restricting access on our computer systems through use of passwords (including procedures around password security), control of access rights and keeping information hidden from outside sight
- ensuring appropriate procedures are used for the transfer of personal data including the use of secure web portals and secure transfer of physical files
- ensuring personal data is not stored on laptops apart from in exceptional circumstances and that personal data stored on paper files is held securely. All data is encrypted when stored on laptops and transferred to the network upon return to head office
- having appropriate facilities in place for disposal of confidential waste
- keeping audit logs in relation to read access, changes, additions, deletions on ICT network
- having an acceptable use of resources policy and a mobile device policy in place.

Principle 6 *(Continued)*

- inserting appropriate data protection and confidentiality clauses in arrangements with any processors of personal data on our behalf, including
  a) the conditions under which data may be processed
  b) the minimum security measures that the data processors must have in place
  c) mechanisms or provisions that will enable the data controller to ensure that any data processor is compliant with the security practices which include a right of inspection or independent audit;
  d) retention/disposal: in general, the retention periods for data defined in our policy are based on the legislative provisions pertaining to the area involved, audit requirements and principle 5.

While ultimately the Data Controller is responsible in law for the security of personal information, it is a responsibility shared with every staff member.

Accountability

Responsibility of our employees

All employees of the Office have a duty to ensure compliance with the principles of Data Protection and undertake to follow the provisions of this Code of Practice in accordance with our stated policy and procedures.

Each employee is charged with the responsibility of ensuring that any data that they access, manage and control as part of their daily duties is carried out in accordance with the General Data Protection Regulation and Irish data protection legislation and this Code of Practice.

Employees found in breach of the Data Protection rules may be found to be acting in breach of or, in certain circumstances, committing an offence under the General Data Protection Regulation and Irish data protection legislation. In addition, the Official Secrets Act 1963 provides for sanctions and fines in relation to breaches of confidentiality of information. All current and former employees of the Office may be held accountable in relation to all data processed, managed and controlled by them during the performance of their duties in the Office.

Managers have a particular responsibility to train staff and ensure that they are aware of and meet the requirements of the Office's data security policies. We will ensure that information to allow staff and managers to fully comply with this Code of Practice is provided on our intranet. We have put in place training programmes to help both staff and managers to achieve this aim.

Data governance arrangements

We have established a Security Forum to oversee the information security and data protection process in the Office. The Forum comprises the Secretary and Director of Audit, other senior management and other staff within the Office. We have assigned responsibility for data protection to a Data Protection Officer (DPO) who reports to the Forum. The DPO's role is to:

- maintain and update the data protection register for the Office
- manage any data subject access requests
- manage any data security breaches or data loss incidents
- provide advice and assistance for staff on data protection issues and where necessary commission legal advice
- oversee the provision of data protection training and guidance for staff
- maintain and update the data protection policy and associated documentation
- advise the management team on compliance with the legislation
- manage personal data audits if required by the management team.

To ensure the quality of data retained by the Office, and that access to and usage of such data is appropriate within the terms of this Code, we will conduct examinations and reviews of Data Protection procedures as part of our on-going compliance process.

Risks associated with the storage, handling and protection of personal information are handled through our risk management process.

Furthermore, external audits of all aspects of Data Protection within the Office may be conducted on a periodic basis by the Data Protection Commission.

Protocol for Reporting Breaches

A data breach is defined as personal data that has been put at risk of unauthorised disclosure, loss, destruction or alteration whether in manual or electronic form. These could include inappropriate access to personal information on the Office's systems or the sending of personal information to the wrong individual.

If any breaches of the code of practice or of the statutory requirements of the General Data Protection Regulation and Irish data protection legislation are committed, our Breach Management Plan must be followed. The Office's Data Protection Officer must be notified where a breach occurs. Where a data breach has occurred the Data Protection Commission must be notified without undue delay and within 72 hours of becoming aware of the breach.

Registration

The Office is registered as a Data Controller under Irish data protection legislation. We provide annually, a list of personal data holdings and data exchanges made under national legislation, EU and other binding international agreements to the Data Protection Commission.

Appendix 1

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the code of practice

The Data Protection Act 2018 – Irish data protection legislation confers rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All staff in the organisation must comply with the provisions of Irish data protection legislation when collecting and storing and working with personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation.

Data - Information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Relevant Filing Systems - Any set of information organised by name, PPSN (if applicable in an organisation), payroll number, employee number or date of birth or any other unique identifier would all be considered relevant.

Personal Data - Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Access Request - This is where a person makes a request to the organisation for the disclosure of their personal data.

Data Processing - Performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data;
- Collecting, organising, storing, altering or adapting the data;
- Retrieving, consulting or using the data;
- Disclosing the data by transmitting, disseminating or otherwise making it available;
- Aligning, combining, blocking, erasing or destroying the data.

Data Subject - An individual who is the subject of personal data.

Data Controller - A person who (either alone or with others) controls the contents and use of personal data.

Data Processor - A person who processes personal information on behalf of a data controller, but does not include a data controller who processes such data in the course of his/her employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Irish data protection legislation places responsibilities on such entities in relation to their processing of the data.

Appendix 2

Enforcement of Data Protection Legislation

Role of the Data Protection Commission

The Irish data protection legislation established the independent office of the Data Protection Commission. The Commission is appointed by Government and is independent in the performance of its functions. The Data Protection Commission's function is to ensure that those who keep personal data in respect of individuals comply with the provisions of the General Data Protection Regulation and Irish data protection legislation.

The Commission maintains a register, available for public inspection, giving general details about the data handling practices of a range of data controllers, such as Government Departments, state agencies and financial institutions.

The Data Protection Commission has a wide range of enforcement powers to assist in ensuring that the principles of Data Protection are being observed. These include the serving of legal notices compelling a data controller to provide information needed to assist his/her enquiries, compelling a data controller to implement a provision in the Irish data protection legislation, etc.

The Data Protection Commission also investigates complaints made by the general public in relation to personal data and has wide powers in this area. For example, the Commission may authorise officers to enter premises and to inspect personal information held on computer or relevant paper filing systems. Members of the public who wish to make formal complaints may do so by writing to the Office of the Data Protection Commission, Canal House, Station Road, Portarlington, Co. Laois, or by email to info@dataprotection.ie.

Where any employee, in the normal course of his or her duties, becomes aware that an individual, including employees of the Office may be breaching the Irish data protection legislation or have committed or are committing an offence, they should report the matter to the Data Protection Officer. The Audit Board has delegated authority to the Deputy Director Corporate Services as Data Controller for the Office. A data controller found guilty of an offence under the Irish data protection legislation can be fined amounts up to €50,000 on conviction and/or may be ordered to delete all or part of a database if relevant to the offence.

Useful Contacts

Advice/Assistance

All requests for advice and assistance on data protection issues within the Office should be directed to the Data Protection Officer at the contact address below.

Applying for Access to Personal Data

Requests for personal data should be made in writing to:

Data Protection Officer
Office of the Comptroller and Auditor General
3A Mayor Street Upper
Dublin 1
D01PF72
Phone (01) 863 8600 or email dpo@audit.gov.ie

Responding to Requests

When a valid request is received the Office must reply within 30 days, even if personal data is not held.

Further Information

Data Protection Commission
Phone: 1890 252231
http://www.dataprotection.ie info@dataprotection.ie

Protection of Personal Data

Code of Practice