Oifig an Ard-Reachtaire Cuntas agus Ciste
Office of the Comptroller and Auditor General

Data Protection Policy

“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. **Lawfulness, fairness and transparency**
2. **Purpose limitation**
3. **Data minimisation**
4. **Accuracy**
5. **Storage limitation**
6. **Integrity and confidentiality**

Table of Contents

Introduction

The General Data Protection Regulation (GDPR) 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 the Office of the Comptroller and Auditor General collects and holds 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. We have been given statutory right of access to data and information to ensure that we are effective in the discharge of our statutory functions. Some of the records and the related information that we are granted access to may contain personal information.

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 GDPR, 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 policy 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 Policy

Purpose

Set against the GDPR and Irish data protection legislation the aim of the Data Protection Policy 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 Policy applies to all records generated or obtained by the Office, which contain personal information relating to living 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.

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.

Data Protection Principles

There are six key data protection principles set out in Article 5 of the GDPR.

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality.

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

Principle 1 – lawfulness, fairness and transparency

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

Article 6 of the GDPR sets out the circumstances under which the processing of personal data is considered to be lawful. These are

- the data subject has given consent to the processing of his or her personal data
- processing is necessary for the performance of a contract
- processing is necessary for compliance with a legal obligation to which the data controller is subject
- processing is necessary in order to protect the vital interests of the data subject or of another person
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party.

Our Website Privacy Notice, available on the Office website, identifies the ways in which we collect, hold and process personal data, the lawful basis for that processing and the type of personal data that we handle.

In summary, we collect, hold and process data in accordance with our statutory functions of audit, examination and inspection, as a prescribed person under protected disclosures legislation, in connection with 'audit insights' events or in relation to the administrative operations of the Office.

An audit involves accessing and testing a variety of information. Section 10 of the Comptroller and Auditor General (Amendment) Act 1993 gives audit staff the authority to request information and explanations necessary for the purpose of our work. This may involve collecting and processing personal data, for example payments by audited bodies to individuals.

Principle 1

(continued)

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. Personal data requests for audit, inspection or examination purposes will be requisitioned in accordance with an audit plan or scope of an examination and approach authorised by a manager.

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)).

We only collect personal data for specific, explicit and legitimate purposes. 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.

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 do not give personal information 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 GDPR 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 policies and 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.

To comply with this principle, we limit the personal data collected to what is required to fulfil a specific purpose.

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 network or the Office's ICT network (and in accordance with the requirements in the Office's Information and Data Security Policy with regard to its retention within the Teammate+ application, where applicable)
- 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 its accuracy.

The Office is the data controller for the personal data that it processes. 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.

This principle has limited applicability in the exercise of our statutory audit, examination and inspection functions. This is to ensure that the C&AG is not materially restricted in his ability to carry out those functions (Section 60(3)(c)(iii) of the Data Protection Act 2018 Act).

Principle 5 - storage limitation

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.

The National Archives Act 1986 and regulations in 1988 are the principle statutes applicable to the management, disposal or retention of records of Departments of State, including those of our Office. No legislation takes precedence over the Act with regard to the management of public records.

We have a Records Management Policy which identifies the retention period for records falling in certain series corresponding to the main business functions of the Office.

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 National Archives legislation. We aim to destroy records relating to audits and examinations, in accordance with the legislation and our Records Management Policy.

Principle 6 - integrity 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. To that end we have appropriate security measures in place which include, inter alia,

- maintaining ISO 27001 Information Security Management System 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
- ensuring caution is exercised when transporting equipment and files between locations
- 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 all staff connect to the Office network through direct access machines or through Citrix and that no personal data is stored on laptops
- ensuring personal data stored on paper files is held securely while not in use, preferably in a locked cabinet and access restricted to only those persons with business reasons to access them
- having appropriate facilities in place for disposal of confidential waste
- keeping audit logs in relation to read access, changes, additions, deletions on ICT network

Principle 6 *(continued)*

- having an ICT acceptable usage policy and a laptop policy and USB storage device policy in place to ensure all staff are fully aware of their obligation in terms of access to and use of official ICT services
- having a social media policy (within the Offices ICT Policy) which reminds staff of the requirements and the restrictions under the Official Secrets Act 1963
- 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 Office to ensure that any data processor is compliant with the security requirements which include a right of inspection or independent audit
d) retention/disposal: in general, the retention periods for data defined in our Records Management Policy are based on the legislative provisions pertaining to the area involved, audit requirements and principle 5.

Accountability

Data subject rights

A data subject, under the General Data Protection Regulation (GDPR), is an identified or identifiable natural person (an individual) whose personal data is being processed.

This means you are a data subject if a company or organisation holds or uses any information that relates to you, such as your name, location, or online identifier. As a data subject, you have rights under the GDPR, including the right to be informed about your data, the right to access and rectify it, and the right to have it erased. The term only relates to people who are alive. Data protection law doesn't apply after someone has died.

Responsibility of our employees

While the Office, as data controller, is ultimately responsible in law for the protection of personal data, all employees have a duty to ensure compliance with the principles of data protection and adhere to our data security policies.
Each employee is charged with the responsibility of ensuring that any personal data that they access, manage and control as part of their daily duties is carried out in accordance with the GDPR and Irish data protection legislation and this Data Protection Policy.
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 GDPR 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.
To assist employees in complying with their responsibilities in relation to data protection the following actions are taken

- our data security policies are available to all staff on the Office intranet
- all staff are provided with appropriate training on data security and data protection
- managers are made aware of their responsibility to train staff and ensure that they are aware of and meet the requirements of the Office's data security policies
- all staff are asked to include a standard goal relating to compliance with data security policies on their role profile forms as part of the PMDS process
- staff need to sign off on compliance in each audit file in TeamMate+.

Role and responsibility of the Data Protection Officer

Monitoring compliance

A Data Protection Officer (DPO) monitors an organisation's adherence to GDPR and other data protection laws, relevant policies, and the assignment of responsibilities for data protection within the company.

Information and advice

They inform and advise the organisation, its employees, and processors about their obligations under data protection laws and assist in raising staff awareness and providing training.

Data Protection Impact Assessments

The DPO provides advice when a Data Protection Impact Assessment (DPIA) is required and monitors its performance.

Contact point

The DPO serves as the primary contact point for individuals (data subjects) regarding their rights and for the relevant supervisory authority on all data protection issues.

Incident management

They play an active role in data breach management, including reporting to the supervisory authority and containing the incident.

Responsibility of the Office of the Comptroller and Auditor General

Maintain a Record of Processing Activities (ROPA)

The Office has appropriate policies and procedures around data protection, information security, access control and records management in demonstrating our accountability for data protection and compliance with our obligations under data protection legislation. Article 30 of the GDPR requires Data Controllers to maintain a Record of Processing Activities (RoPA) under their responsibility. Article 30 GDPR prescribes the information the records must contain and states that controllers and processors must be in a position to provide such records to the Data Protection Commission (DPC) on request. The RoPA, as a measure to demonstrate compliance, is one of the means by which Data Controllers demonstrate and implement the principle of accountability as set out in Article 5(2) GDPR. A well drafted RoPA will demonstrate to the DPC that a Data Controller is aware of, and has considered the purpose of, all processing activities taking place within the organisation.

Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR.

In complying with GDPR responsibilities, the Office will take into account the costs of the implementation and the nature, the scope, context and purpose of the processing together with the risk of varying likelihood and severity for the rights and freedoms of the data subject. The security measures implemented should where possible prevent a breach and where a breach occurs allow a timely response.

The Office maintains a corporate risk register that is reviewed quarterly during the meeting.

Data protection by design and by default

Articles 25(1) and 25(2) of the GDPR outline our obligations concerning data protection by design and by default.
Privacy by Design means that the office considers privacy at the initial design stages and throughout the complete development process of new products, processes or services that involve processing personal data.

Privacy by Default means that when a system or service includes choices for the individual on how much personal data they share with others, the default settings should be the most privacy friendly ones. This means the Office integrates data protection into our processing activities and business practices, from the design stage right through the lifecycle.

Third party agreements

We treat all personal data received as confidential and use such data only for the purposes that it was obtained. However, we may share data with third parties, such as other government departments or public authorities, when permitted or required by a specific legislative provision. We may share personal data when necessary for the performance of the Office of its functions and where third parties are providing services for us.
All transfers will be done within the requirements of data protection legislation.

International transfers

The Office will not ordinarily transfer personal data outside of the European Economic Area or third countries. In the event that this position changes, we will comply with our obligations under Article 46 of GDPR by adopting one of the appropriate measures approved by the Data Protection Commission and the European Commission to ensure that such transfers are lawful.

Data governance arrangements

The Office has the following governance arrangements in place to ensure compliance with the data protection requirements

- ***Information Security Forum*** – we have established an Information Security Forum to oversee information security and data protection processes in the Office.
- ***Data Protection Officer*** – we have assigned responsibility for data protection to a Data Protection Officer with the Information Security Forum having oversight of this role.
- ***Risk Management process*** – risks associated with the storage, handling and protection of personal information are handled through our risk management process.
- ***Data security arrangements*** – we ensure that appropriate controls are in place to meet the requirements of the information security standard ISO 27001. Independent audits of our information security management system including surveillance audits by the ISO certification body, are regularly carried out.
- ***Examination and reviews of data protection*** – 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 Policy, we will conduct examinations and reviews of data protection procedures as part of our on-going compliance process.
- ***External accountability*** – external audits of all aspects of data protection within the Office may be conducted 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. This could include inappropriate access to personal information in the Office's systems or the sending of personal information to the wrong individual.

If any breaches of the Data Protection Policy or of the statutory requirements of the GDPR and Irish data protection legislation are committed, our *Data Breach Policy and our Security Incident/Data Breach Reporting procedure* must be followed. The Office's DPO must be notified where a breach occurs. Where a risk to the rights and freedoms of the data subject is deemed to exist the Office must inform the Data Protection Commission without undue delay and within 72 hours of becoming aware of the breach.

Appendix 2 provides information on the role of the Data Protection Commission and its powers.

Appendix 1

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the Data Protection Policy

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

The 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 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 Data
Protection Commission, 6 Pembroke Row, Dublin 2, D02 X963 Ireland or online via their website.

The Commission has power to impose an administrative fine of up to one million euro on public sector bodies found to have infringed the data protection requirements.

Appendix 3

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 using the contact details below.

Data Protection Officer
Office of the Comptroller and Auditor General 3A Mayor Street Upper
Dublin 1 D01 PF72
Phone (01) 863 8600 or email dpo@audit.gov.ie

Further Information
Data Protection Commission