An Roinn Cultúir,
Oidhreachta agus Gaeltachta
Department of Culture,
Heritage and the Gaeltacht

Department of Culture, Heritage and the Gaeltacht

Data Protection Policy

Corporate Governance

May 2018

Contents

Introduction from the Secretary General

This Data Protection Policy is a statement of the Department of Culture, Heritage and the Gaeltacht's commitment to protecting the rights and privacy of individuals in accordance with the EU General Data Protection Regulation and the Data Protection Acts 1988 to 2018.

In collecting personal data, the Department has a responsibility to use it both effectively and ethically, taking into consideration both the individual's right to privacy and the Department's legitimate business requirements. We are therefore committed to ensuring that the collection, processing and storage of data in the course of our business is conducted in a safe, secure and lawful manner in compliance with all relevant data protection legislation.

Set against the General Data Protection Regulation and the Data Protection Acts, this Data Protection Policy will provide a basis for all employees of the Department to develop their understanding of the concepts of data protection and an awareness of their individual responsibilities in this regard. This will, in turn, enable the Department to meet its legal obligations in respect of data protection legislation across all areas of its operations.

Katherine Licken
Secretary General

1. Foreword

The mission of the Department of Culture, Heritage and the Gaeltacht (DCHG) is:

"To promote, nurture and develop Ireland's arts, culture and heritage; to support and promote the use of the Irish language, and to facilitate the development of the Gaeltacht and Islands."

The Department is committed to protecting the rights and privacy of individuals in accordance with both European Union and Irish data protection legislation as set out in the Data Protection Acts 1988 to 2018. The Department is required to lawfully and fairly process personal data about employees, customers, suppliers and other individuals in order to achieve its mission and functions.

Data Protection legislation confers rights on individuals as well as responsibilities on those persons processing personal data. This policy sets out how the Department seeks to process personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work.

The EU General Data Protection Regulation (GDPR EU 2016/679), which came into effect on 25th May 2018, replaced the Data Protection Directive 95/46/EC and is designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organisations across the region approach data privacy.

2. Purpose

This Data Protection Policy applies to all staff of the Department of Culture, Heritage and the Gaeltacht, both permanent and temporary, to staff working on a contract basis for the Department, and others who are authorised to access personal data held by the Department. This policy should be read in conjunction with other relevant Departmental policies and procedures. The Department may supplement or amend this policy by additional policies and guidelines from time to time.

This Data Protection Policy is a statement of the Department's commitment to protect the data protection rights of individuals in accordance with all relevant legislative requirements.

3. Scope

This policy applies to all of the Department's personal data processing functions in relation to identified or identifiable natural persons, including those performed on customers, employees, suppliers, and any other personal data the Department processes from any source.

Personal data is defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data is defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, 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.

4. Data Protection Principles

All processing of personal data must be conducted in accordance with the data protection principles set out in relevant legislation. The Department's policies and procedures are designed to ensure compliance with the following principles:

4.1 'Lawfulness, fairness and transparency'

Personal data shall be processed **lawfully, fairly and in a transparent manner** in relation to the data subject.

4.2 'Purpose limitation'

Personal data shall be 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, in accordance with Article 89(1) of the GDPR, not be considered to be incompatible with the initial purposes;

4.3 'Data minimisation'

Personal data shall be **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;

4.4 'Accuracy'

Personal data shall be **accurate and, where necessary, kept up-to-date**. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

4.5 'Storage limitation'

Personal data shall be 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 in accordance with Article 89(1) of the GDPR, subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject;

4.6 'Integrity and confidentiality'

Personal data shall be 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.

5. Rights of data subjects

The Department will design and maintain appropriate policies, procedures and training to implement the following data rights of data subjects:

5.1 Right of access by the data subject

The Department will implement procedures to ensure that requests from data subjects for access to their personal data will be identified and fulfilled in accordance with the legislation. Further information can be found here and at *Appendix 3* and *4*.

5.2 Right to rectification

The Department is committed to holding accurate data about data subjects and will implement processes and procedures to ensure that data subjects can rectify their data where inaccuracies have been identified.

5.3 Right to erasure (right to be forgotten)

The Department will only process personal data where there is a lawful basis for doing so. Where the Department receives requests from data subjects looking to exercise their right to erasure, the Department will then carry out an assessment of whether the data can be erased without affecting the ability of the Department to provide future benefits and services to the data subject, and taking into account the Department's legal obligations under the National Archives Act 1986.

5.4 Right to restriction of processing

The Department will assess whether a data subject's request to restrict the processing of their data can be implemented.

5.5 Right to data portability

The Department will only process personal data where there is a lawful basis for doing so. Where the Department has collected personal data on data subjects by consent or by contract, the data subjects then have a right to receive the data in a structured, commonly used and machine-readable format and have the right to transmit that data to another data controller.

5.6 Right to object

Data subjects have a right to object to the processing of their personal data in specific circumstances, as outlined in Article 21 of the GDPR. Where such an objection is received, the Department will assess each case on its merits.

5.7 Right not to be subject to automated decision-making

Data subjects have the right not to be subject to a decision based solely on automated processing, where such decisions would have a legal or significant effect concerning him or her. The Department will ensure that where systems or processes are implemented that calculate benefits or services, that an appropriate right of appeal is available to the data subject.

5.8 Right to complain

The Department will operate a complaints process whereby data subjects will be able to contact the Data Protection Officer (DPO). The DPO will work with the data subject to bring the complaint to a satisfactory conclusion for both parties. The data subject will be informed of their right to bring their complaint to the Data Protection Commission.

6. Responsibility for this policy

The Department is committed to compliance with all relevant EU and Irish laws in respect of personal data, and the protection of the rights and freedoms of individuals whose information the Department controls and processes.

All staff working in the Department, and third parties working on behalf of the Department who separately collect and/or control the content and use of personal data, have responsibility for ensuring that personal data is collected, stored and handled appropriately. It is the responsibility of the Heads of each Business Unit that handles personal data to ensure it is handled and processed in line with this policy, best practice and data protection legislation.

7. Responsibilities of the Department

The Department has responsibility for the following:

7.1 Maintaining a record of data processing

The Department will maintain a record of data processing activities (ROPA) in the manner prescribed by Article 30 of the GDPR. To ensure data accuracy, the record will be reviewed by the Heads of each Business Unit on an annual basis and a report will be subsequently submitted to the Management Board for information purposes.

7.2 Ensuring appropriate technical and organisational measures

The Department will implement appropriate technical and organisational measures to ensure and be able to evidence that personal data is protected.

7.3 Implementing appropriate agreements with third parties

The Department will implement appropriate agreements and contracts with all third parties with whom personal data is shared. The term ‘third parties’ includes other departments and agencies of the Irish Government. All such agreements shall be implemented in writing prior to the commencement of the transfer of the data. The agreement shall specify the purpose of the transfer, the requirement for adequate security, right to terminate processing, restrict further transfer to other parties, and ensure that response will be given to requests for information and the right to audit.

7.4 Transfers of personal data outside of the European Economic Area (EEA)

The Department will not transfer the personal data of its data subjects outside of the EEA unless appropriate safeguards are in place.

7.5 Data protection by design and default

Prior to the time of determining the means of processing and also during the processing, the Department will ensure that appropriate technical and organisational measures and safeguards are integrated into the process and that they adhere to the data protection principles.

7.6 Data Protection Impact Assessments (DPIAs)

Where any new types of processing, in particular using new technologies, result in a high risk to the rights and freedoms of its data subjects, the Department shall carry out a Data Protection Impact Assessment (DPIA). As part of this process, a copy of the impact assessment shall be shared with the Department's Data Protection Officer. Where the Department is unable to identify measures that mitigate the high risks identified, it will consult with the Data Protection Commission prior to the commencement of processing.

7.7 Personal data breaches

A 'personal data breach' is defined under *Appendix 1* as meaning a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The Department has developed a protocol for dealing with personal data breaches, which includes the methodology for handling a personal data breach and for notification to the DPC and data subjects where necessary.

7.8 Freedom of Information

The Freedom of Information (FOI) Act 2014 obliges the Department to publish information on their activities and to make the information held, including personal information, available to citizens and customers.

The Department will operate procedures to ensure that requests for personal data are correctly fulfilled under either data protection legislation or FOI legislation.

7.9 Governance

The Department will monitor compliance with relevant legislation through a Data Protection Working Group. The working group of staff will be nominated by the Heads of each Business Unit within the Department, and designated to assist the Data Protection Officer with a range of data protection matters on an ongoing basis.

8. Responsibilities of the Data Protection Officer

Data Protection Officer

Under Article 37 of the GDPR, all public bodies are required to appoint a Data Protection Officer (DPO). The DPO will report to the Management Board and their responsibilities include the following:

a) Keeping the Management Board and Data Protection Working Group updated about data protection responsibilities, risks and issues;

b) Acting as an advocate for data protection within the Department;

c) Monitoring compliance with the relevant data protection legislation;

d) Reviewing and updating, as appropriate, all of the Department's data protection policies on a regular basis;

e) Communicating the Department's data protection policies to, and organising appropriate data protection training and advice for, all staff members and those included in this policy;

f) Providing advice where requested as regards the Data Protection Impact Assessments and monitoring that such assessments are completed to an appropriate standard;

g) Providing advice on data protection matters from staff, board members and other stakeholders;

h) Responding to individuals, such as clients and employees, who wish to exercise their data protection rights;

i) Liaising with the Heads of each Business Unit to ensure that appropriate data processing agreements are put in place with third parties that handle the Department's data, and ensuring that reviews of third parties are carried out on a regular basis;

j) Ensuring that the record of data processing is updated as necessary;

k) Acting as a contact point and providing cooperation with the Data Protection Commission.

Registration with the Data Protection Commission

Under the Data Protection Acts 1988 to 2018, certain categories of data controllers (those who control the contents and use of personal data) and certain categories of data processors (those whose business consists wholly or partly in processing such data for others) must register with the Data Protection Commission (DPC). The register of data controllers and processors is a public register intended to bring transparency to the

processing of personal data. All register entries are available on the DPC website www.dataprotection.ie

A full list of data held and/or processed by the Department of Culture, Heritage and the Gaeltacht is available on the DPC website and at *Appendix 2* of this policy.

While the Head of 'Corporate Governance and Services' is the Data Controller for the purposes of registration with the DPC, each Head of Unit is responsible for the protection of personal data within their own areas of operation.

9. Responsibilities of staff

Anyone who processes personal data on behalf of the Department has a responsibility to comply with this Data Protection Policy.

9.1 Training and Awareness

All staff will receive appropriate training relating to the GDPR, data protection and records management. New staff will receive training as part of the induction process.

All staff will be kept aware of data protection obligations through regular notifications from the Data Protection Office and poster campaigns.

9.2 Failure to comply with the data protection policy

All staff have a duty to ensure compliance with the principles of data protection and undertake to follow the provisions of this policy. All staff are charged with the responsibility to ensure that all data processed by them as part of their daily duties is done in accordance with Data Protection legislation and this policy. Breaches of this policy may result in disciplinary action.

10. Queries about the Data Protection Policy

The Department has further information relating to data protection on its website, which you can refer to here.

Further questions or concerns about the Department's personal data policies should be directed to the Data Protection Officer at:

Data Protection Officer
Department of Culture, Heritage and the Gaeltacht
23 Kildare Street
Dublin 2
D02 TD30

Email: data.protection@chg.gov.ie

Appendix 1

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

The Data Protection Acts – The Data Protection Acts 1988 to 2018 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All Department staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the Department and individuals who interact with the Department.

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 a 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).

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.

Special categories of personal data – Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, 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.

Relevant filing system – Any set of information organised by name, PPS Number, payroll number, employee number, date of birth, or any other unique identifier, would all be considered relevant.

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.

Access Request – Where an individual makes a request to the organisation for the disclosure of their personal data under Data Protection legislation.

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, e.g. an employee of an organisation to which the data controller outsources work. The Acts place responsibilities on such entities in relation to their processing of the data. Note: A data processor does not refer to an employee of a data controller.

Personal Data Breach – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Appendix 2

List of information held by the Data Protection Commission on the public list of registrations

Purpose:

The mission of the Department of Culture, Heritage and the Gaeltacht is:

"To promote, nurture and develop Ireland's arts, culture and heritage; to support and promote the use of the Irish language, and to facilitate the development of the Gaeltacht and Islands."

In this regard, the Department aims to carry out all lawful and administrative functions of the Minister for Culture, Heritage and the Gaeltacht in relation to the processing of personal data relating to all aspects of the Department's business.

Description:

All purposes associated with the discharge of the functions of the Department to include:

- General Administration (telephone directories, contact lists, circulation lists, email addresses, car registration details for parking, CCTV footage – kept for 28 days);
- IT Services and Applications (email addresses, staff numbers);
- Financial and Personnel Management (details of employees, salaries, deductions, work history, CV's, departmental payee details as necessary including grantees and personal details as appropriate);
- Programmes, grants, processes and procedures in relation to the Culture Section (applicant details and records as requested in the application process);
- Programmes, grants, processes and procedures in relation to the Heritage Section (applicant details and records as requested in the application process, planning applications, licensee applications and other processes in relation to the Heritage Section);
- Programmes, grants, procedures and processes in relation to the Gaeltacht Section (applicant details and records as requested in the application process);
- Details of Board members on the Bodies under the Department's aegis (contact details, CV's, bank details for payment of fees/expenses);
- FOI (contact details of applicants);
- Licensing, certification and authorisations appropriate to the Department;
- Details relating to public consultation processes.

Disclosees:

- Minister for Culture, Heritage and the Gaeltacht, and such other Ministers as may be assigned responsibility for Departmental functions or where necessary and appropriate;
- Members of the Oireachtas in the performance of their representative and parliamentary duties;
- Government Departments/Offices;
- State Agencies;
- Office of the Revenue Commissioners;
- Pensions Board;
- Comptroller and Auditor General
- National Shared Services Office
- Computer maintenance personnel;
- An Garda Síochána;
- Offices of the Information Commissioner and Data Commission;
- Chief State Solicitors Office and Attorney General;
- Freedom of Information – release of data under the FOI Acts;
- Departmental website – data in relation to certain aspects of the Department's work is available on the website as appropriate;
- Authorised staff – personal data is available to authorised staff only and this is protected by limited access to files.

Transfers Abroad:

None

Appendix 3

Enforcement of Data Protection Legislation

Data Protection Commission

The Data Protection Commission (DPC) was established by the Data Protection Acts 1988 to 2018. The Commission shall be the supervisory authority and is responsible for monitoring the lawfulness of processing of personal data in accordance with Data Protection legislation. All functions that were vested in the Data Protection Commissioner have now been transferred to the Commission.

The Commission shall consist of no more than 3 members, as the Government determines. Each member of the Commission shall be known as a Commissioner for Data Protection.

The tasks of the Commission include promoting public awareness and understanding of the risks, rules, safeguards and rights in relation to processing, handling complaints lodged by data subjects, and cooperating with (including sharing information with) other data protection authorities in other EU Member States.

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 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 their enquiries, compelling a data controller to implement a provision in the Act etc.

The Commission also investigates complaints made by the general public in relation to how their personal data is processed by an organisation. For example, the Commission may authorise officers to enter premises and to inspect personal information held on computer or relevant paper filing system. Further information about raising potential concerns or infringements of your data protection rights can be found here.

Where the Commission decides to impose an administrative fine on a controller or processor that is a public authority or a public body, the amount of the administrative fine concerned shall not exceed €1,000,000.

Applying for Access to Personal Data

Under Data Protection legislation, individuals have a right to obtain from the Department of Culture, Heritage and the Gaeltacht, a copy of any personal information held on them on computer or structured filing system. This is commonly referred to as a Subject Access Request.

In order to obtain copies of personal data held by the Department, a request must be made in writing to the below address seeking the information:

Data Protection Officer
Department of Culture, Heritage and the Gaeltacht
23 Kildare Street
Dublin 2
D02 TD30

Email: data.protection@chg.gov.ie

Further information on the right of access, including a Subject Access Request form, can be found here.

Responding to Access Requests

When a valid request is received, the Department must reply within one month, even if personal data is not held. Where requests are complex or involve a large number of requests, this time limit may be extended for a further two months.

There is no fee applicable to making an access request for your own personal data, unless the request is considered manifestly unfounded or excessive.

Some exceptions apply to the release of data, including access to third party data, legally privileged data, or data required for the prevention, investigation or prosecution of criminal offences.

Section 61(1) of the Data Protection Act 2018 also allows for restrictions on the exercise of the rights of data subjects where processing is for archiving purposes in the public interest.

Appendix 4

Departmental Privacy Statement

The Department of Culture, Heritage and the Gaeltacht is committed to protecting and respecting your privacy and employs appropriate technical and organisational measures to protect your information from unauthorised access. The Department will not process your personal data for any purpose other than that for which they were collected. Personal data may be exchanged with other Government Departments, local authorities, agencies under the aegis of the Department, or other public bodies, in certain circumstances where this is provided for by law.

The Department will only retain your personal data for as long as it is necessary for the purposes for which they were collected and subsequently processed. When the business need to retain this information has expired, it will be examined with a view to destroying the personal data as soon as possible, and in line with Department policy. Further information on Data Protection can be found on our website at: https://www.chg.gov.ie/help/legal-notices/data-protection/