Protection of Personal Data

Code of Practice

Revenue
Cáin agus Custaim na hÉireann
Irish Tax and Customs

RPC001147_EN_D_19

Table of Contents

Data Protection Rules

There are specific requirements and responsibilities that our organisation must follow, described by the Data Protection Commissioner as the “8 Rules”:

Rule 1	**Obtain and process information fairly**
Rule 2	**Keep it only for one or more specified and lawful purpose(s)**
Rule 3	**Process it only in ways compatible with the purposes for which it was given initially**
Rule 4	**Keep it safe and secure**
Rule 5	**Keep it accurate and up-to-date**
Rule 6	**Ensure that it’s adequate, relevant and not excessive**
Rule 7	**Retain it no longer than is necessary for the specified purpose(s)**
Rule 8	**Give a copy of his/her personal data to any individual, on request**

Tear along perforation and retain this for reference

Foreword

I am very happy to be able to formally approve this Code of Practice under the terms of Section 13 of the Data Protection Acts 1988 and 2003. The Code is the result of intensive work by Revenue and its staff, working in close co-operation with my Office. It is designed to give operational meaning to the principles of data protection set out in European and National law.

I am confident that the Code will make a significant contribution to improving knowledge and understanding of data protection within Revenue. I intend to continue to work closely with Revenue and its staff to ensure that the guidance set out in the Code is followed in daily practice.

Billy Hawkes

Data Protection Commissioner

Introduction

Information is at the core of Revenue's business. The security and protection of personal information that Revenue holds is of critical importance to our customers and therefore to the organisation. The public expect Revenue staff to treat their tax, business, and personal information with the greatest possible care and to ensure that it will be accessed by Revenue staff only when necessary for the purposes of dealing with their Revenue affairs.

It is vitally important to maintain Revenue's good record in relation to safeguarding confidential data and the confidence of the public. 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 Data Protection Acts 1988 and 2003, Section 77 of the Finance Act 2011 (Confidentiality of Taxpayer Information), the Revenue Code of Ethics 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 taxpayer information held by Revenue. The Code has been approved by the Board.

Signed

Chairman
December 2012

Data Protection Code of Practice

The eight data protection rules

Set against the Data Protection Acts 1988 and 2003 the aim of this Code of Practice is to ensure each employee of Revenue has an understanding of the concepts of Data Protection and is aware of their own responsibilities. This will assist Revenue in its compliance with the Acts. This policy applies to all records generated or obtained by Revenue, 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 Data Protection Acts 1988 and 2003, certain categories of data must be registered with the Data Protection Commissioner.

Revenue customers are entitled to know that their information is being processed for legitimate purposes and disclosed only where permissible by law. Revenue will undertake the following procedures to ensure compliance with the eight principle rules of Data Protection.

Rule 1

Obtain and process information fairly.

"Revenue is 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. Staff will be provided with a list of all relevant legislative provisions. This information will be used to administer the law fairly, reasonably and consistently in seeking to collect no more that the correct amount of tax or duty due".

Rule 2

Keep data for specified, explicit and lawful purposes.

Revenue may only keep data for a purpose(s) that is specific, lawful and clearly stated and the data will only be processed in a manner compatible with this purpose.
Revenue collects a wide range of data for the administration of taxes, duties and customs controls for which it has legal responsibility. These include income tax, VAT, stamp duty, corporation taxes, tax relief and allowances, the customs regime for control of imports and exports and the collection of duties and levies on behalf of the EU. Revenue clearly states the statutory basis and the purpose for which a return is required on all forms issued to the public. The uses of the Personal Public Service Number (PPSN) by Revenue are limited to those of a stated purpose and as provided for in the relevant legislation.

Rule 3

Use and disclose data only in ways compatible with these purposes.

Personal information obtained by Revenue for a particular purpose may not, in general terms, be used for any purpose other than that for which it was obtained. However, Section 872 of the Taxes Consolidation Act 1997 allows any information acquired in connection with any tax or duty to be used by Revenue for any purpose connected with any other tax or duty under Revenue's care. This personal data may not be divulged to a third party except where provided for by law. Revenue reviews and publishes a list of statutory provisions, which allow for the disclosure of taxpayer information. This is made available to staff on the Revenue intranet. For the purposes of the Acts, processing of personal data by contractors on behalf of Revenue 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. Revenue staff are instructed through operating procedures in relation to transfers of data and responsibilities of contractors when handling Revenue data.

Rule 4

Keep data safe and secure.

High standards of physical and technical security are essential to protect the confidentiality of personal data. Revenue has set out the security measures that are in place to do this, including the standard of data security expected of all employees. The highest standards of security are expected. These include, inter alia,

- ensuring access to information is restricted to authorised staff in accordance with a defined policy. Revenue policy ensures that staff access rights extend only to that information necessary to carry out their appointed duties;
- ensuring computer systems are password protected;
- keeping information on computer screens and paper files hidden from callers to offices;
- ensuring that personal data is protected by a high standard of encryption when being stored on portable devices or transferred electronically (including via email);
- ensuring that personal data is not stored on portable devices except in essential circumstances. Where deemed essential, the data must be encrypted and a record kept of the nature and extent of the data and why it is being stored on a portable device. Arrangements should be in place to fully delete the data on the portable device when it is no longer being used;
- having appropriate facilities in place for disposal of confidential waste;
- non-disclosure of personal security passwords to any other individual (including other employees within Revenue);
- keeping premises secure, especially when unoccupied;
- keeping audit logs in relation to read access, changes, additions, deletions on ICT systems;
- having adequate security measures and policies in place in relation to the use of laptops and other mobile storage devices;
- inserting appropriate data protection and confidentiality clauses in arrangements with any processors of personal data on Revenue's behalf, including –

Rule 4 *(Continued)*

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 within Revenue are subject to the legislative provisions pertaining to the area involved. Revenue is obliged by legislative provision to seek authorisation from the Director of the National Archives prior to the destruction of files.

While ultimately the Data Controller is responsible in law for the security of taxpayer information it is a responsibility shared with every officer in the Organisation.

Rule 5

Keep data accurate, complete and up-to-date.

To comply with this requirement, Revenue 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 to eliminate those errors, etc. An officer at Principal Officer level has been assigned responsibility as a Data Controller in Revenue, with designated liaison officers within each of Revenue's divisions;
- every individual has a right to have any inaccurate information rectified or erased. Revenue explains how Data Subjects can interact with the organisation to ensure accuracy of data in each area of its business.

Rule 6

Ensure that data is adequate, relevant and not excessive.

To comply with this rule Revenue has put measures in place to ensure that the information sought and retained is the minimum amount needed for the specified purpose and is adequate, relevant and not excessive in relation to the purpose(s) for which it is kept. These measures are subject to periodic review to assess the continued need for information sought.

Rule 7

Retain data for no longer than necessary for the purpose(s) for which it is acquired.

In general the retention period for data within Revenue is subject to the legislative provisions pertaining to the area involved. For example: Tax record retention should meet the requirements of the Taxes Consolidated Acts whereas Human Resources data would be retained only for as long as permitted by Employer/Employee legislation, amongst others.

We are legally obliged to seek authorisation from the Director of the National Archives in relation to the destruction of all Revenue records that are subject to that legislation.

The capture and retention of CCTV footage will be included in Revenue Retention and Disposal schedules.

Rule 8

Give a copy of his/her personal data to the relevant individual, on request.

Under Section 4 of the Data Protection Acts, on making a written request, with the appropriate fee, any individual about whom Revenue keeps personal information on computer or in a relevant filing system is entitled to (within 40 days):

- a copy of the data being kept about him/her;
- know the purpose(s) for processing his/her data;
- know the identity of any third parties to whom the organisation discloses the data;
- know the source of the data unless this would be contrary to public interest;
- know the logic involved in automated decisions;
- a copy of any data held in the form of opinions expressed about the individual, except where such opinions were given in confidence. The procedure for making a personal data access request is contained in Appendix 2.

If an access request is being refused, the reasons for its refusal must be clearly outlined to the data subject (as per exemptions in Sections 4, 5 and 8 of the Data Protection Acts[1]).

It should be noted that where a request is made to Revenue by, or on behalf of, a person seeking access to their own personal information under the Freedom of Information Act, this request should also be taken as a request under the Data Protection Acts. This is because a valid Data Protection request does not need to refer to the Data Protection Acts. Guidance on how organisations should deal with the overlapping rights of individuals is contained in the Freedom of Information Central Policy Unit Notice Number 23, which is available at http://www.foi.gov.ie/cpu-notices.

[1] Under Section 3 of the Data Protection Acts, an individual has a separate right to be informed, on request, whether an organisation holds personal data on him/her and, if so, to be given a description of the data and the purposes for which they are kept within 21 days of making the request. The restrictions on the right of access to data which are set out in Sections 4 and 5 of the Acts do not apply to the Section 3 right.

Responsibility of Employees of Revenue

All employees of Revenue 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 the organisation's 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 Data Protection Acts 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 Data Protection Acts 1988 and 2003. All current and former employees of Revenue may be held accountable in relation to all data processed, managed and controlled by them during the performance of their duties in Revenue. Section 77 of the Finance Act 2011 increases this accountability and introduces criminal sanctions and fines in relation to breaches of confidentiality of taxpayer information.

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

Audits of data protection and code of practice procedures within Revenue

To ensure the quality of data retained by Revenue, and that access to and usage of such data is appropriate within the terms of this Code, the Internal Audit Unit will conduct examinations and reviews of Data Protection procedures as part of their ongoing examination and review process.

Risks associated with the storage, handling and protection of personal data are included in the Revenue's risk register and risk assessments should take place as part of Revenue's risk strategy.

Furthermore, external audits of all aspects of Data Protection within Revenue may be conducted on a periodic basis by the Office of the Data Protection Commissioner (see www.dataprotection.ie for 2009 audit report).

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 in manual or electronic form on Revenue systems. These could include inappropriate access to personal information on Revenue 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 Data Protection Act are committed, Revenue's Breach Management Plan must be followed. Information in relation to breach notification procedures is available on the Data Protection page of www.Revenue.ie.

Registration

Revenue is registered as a Data Controller under the Data Protection Acts 1988 and 2003. Revenue provides annually, a list of personal data holdings and data exchanges made under national legislation, EU and other binding international agreements to the Office of the Data Protection Commissioner. Further information on the types of information processed by Revenue and disclosees can be viewed on:- http://www.dataprotection.ie/docs/Current_list_of_Registrations_held_by_the_Data_Protection_Co/8.htm

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 Acts - The Data Protection Acts 1988 and 2003 confer 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 the Data Protection Acts 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 under Section 4 of the Acts.

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 an employee of 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 Act 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 Commissioner

The Data Protection Acts established the independent office of the Data Protection Commissioner. The Commissioner is appointed by Government and is independent in the performance of his/her functions. The Data Protection Commissioner's function is to ensure that those who keep personal data in respect of individuals comply with the provisions of the Data Protection Acts.

The Commissioner 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 Commissioner 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 enquiries, compelling a data controller to implement a provision in the Acts, etc.

The Data Protection Commissioner also investigates complaints made by the general public in relation to personal data and has wide powers in this area. For example, the Commissioner 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 Commissioner, Canal House, Station Road, Portarlington, Co. Laois, or by email to info@dataprotection.ie.

Where employees of the organisation, in the normal course of their duties, become aware that an individual including employees of the organisation may be breaching the Acts or have committed or are committing an offence under the Acts, they should report the matter to the Data Protection Unit, Corporate Services Division, Dublin Castle. The Revenue Board has delegated authority to a named Principal Officer as Data Controller for Revenue. A data controller found guilty of an offence under the Acts can be fined amounts up to €100,000 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 organisation should be directed to the Data Protection Unit
Phone - 01-8589160
Email - dataprotection@revenue.ie

Applying for Access to Personal Data

Requests for personal data should be made in writing and accompanied by the requisite fee to:
Revenue
Data Protection Unit
Dublin Castle
Dublin 2
Or email to
dataprotection@revenue.ie

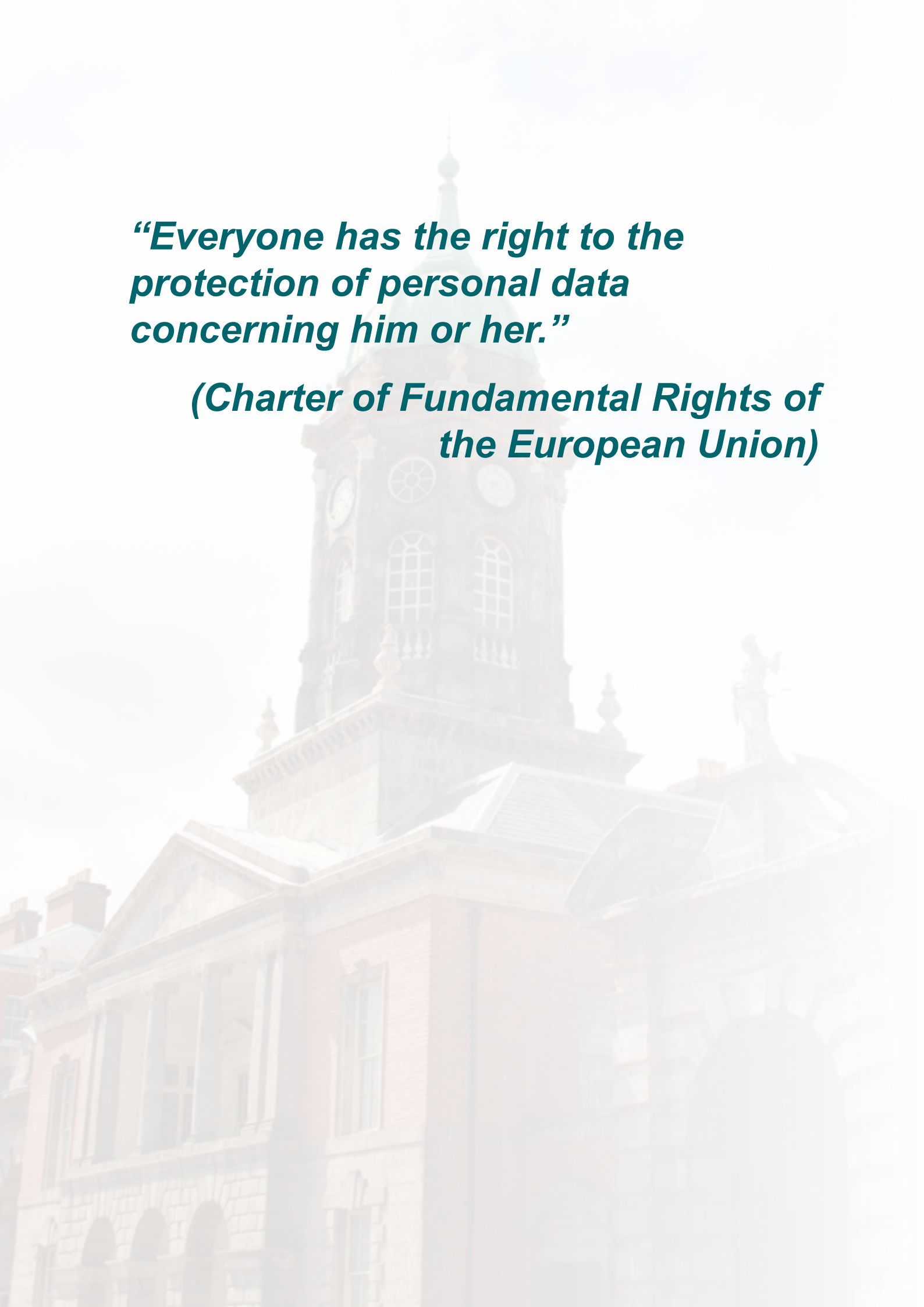
Responding to Requests

When a valid request is received Revenue must reply within 40 days[2] , even if personal data is not held.

Further Information

Data Protection Commissioner's Office,
Phone: 1890 252231,
http://www.dataprotection.ie
info@dataprotection.ie

[2] 21 days if the request is under Section 3 of the Data Protection Acts



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

(Charter of Fundamental Rights of the European Union)

Revenue

Cáin agus Custaim na hÉireann

Irish Tax and Customs

Protection of Personal Data

Code of Practice