

Access Rights and Responsibilities

A guide for Individuals and Organisations

An Coimisinéir
Cosanta Sonraí



Data Protection
Commissioner

This guide is aimed at both individuals and organisations. It is designed to bring individuals through the process of making an access request, and organisations through the process of responding to one.

The guide is laid out in an easy-to-follow question and answer style and covers:

- Accessing Personal Data under the Data Protection Act
- Section 3 - Establishing if an organisation holds personal data about an individual
- Section 4 - Applying for access to a copy of your personal data
- Exemptions and restrictions to the Right of Access
- Section 6 - applying to have personal data corrected, deleted or restricted
- Making a complaint to the Data Protection Commissioner
- How will Access Requests change under GDPR?
- FAQs and definitions
- Check-lists for individuals and organisations

Data Protection is an EU fundamental right for all individuals. All organisations that collect, control or process personal data are required under law to make sure that the data they collect is obtained fairly, stored securely and retained for no longer than is necessary.

The Right of Access is an important right for individuals, allowing them to obtain information about the kinds of data organisations process about them, and to verify that the information is accurate and up to date.

This guide seeks to provide clarity around the rights and obligations that Access Requests cover.

Accessing Personal Data

What rights do individuals have to see what personal data an organisation holds about them?

Under the Data Protection Acts (1988 and 2003) (the Acts) anyone has the right to find out (i) if an organisation holds personal data about them and, if they do, (ii) to apply for a copy of their personal data.

- There are two separate sections under the Acts that deal with individuals applying to see a copy of their own personal data:
 - Section 3 allows an individual to find out if an organisation holds personal data about them.
 - Section 4 allows an individual to make an application for a copy of their personal data.

The difference between the sections, and how to use them, is explained below.

Section 3 – Establishing if an organisation holds personal data about an individual

What does Section 3 entitle an individual to?

- Section 3 of the Acts entitles an individual to make a formal written application to an organisation, asking if they hold any personal data about them.

What is the procedure for making an application?

- Applications under Section 3 must be made **in writing** and should be addressed to the manager or head of the organisation. Some larger organisations will have a Data Protection Officer or a specific address to which applications should be made. (If there is any doubt as to where to send the request, make contact with the organisation first and clarify. Most organisations are very familiar with their obligations under the Acts and will be able to provide the necessary information.) Applicants should keep a copy of the request letter and the date it was sent.

Does an email count as a written request?

- Yes, email is also a valid form when making a Section 3 request. Again, requesters should keep a copy of the email and the date it was sent.

How long does it take?

- Under the Acts, an organisation has **21 days** from the date it receives a Section 3 request to respond with confirmation and a description of the personal data they hold.

Is there a fee?

- No. There is no fee for a Section 3 request.

Are there any conditions?

- The personal data sought must be stored electronically or, for paper records, as part of a structured manual filing system which allows the relevant records to be easily identified.

How to make the process faster?

- Requesters should include any details that will help the organisation locate their personal data, e.g. staff ID numbers, the date-range of the data.

Section 4 – Applying for access to a copy of your personal data

What does Section 4 entitle an individual to?

- Section 4 of the Acts entitles an individual to make a formal written application to an organisation, asking for a copy of any personal data held about them.

What is the procedure for making an application?

- Applications under Section 4 must be made **in writing** and should be addressed to the manager or head of the organisation. Some larger organisations will have a Data Protection Officer or a specific address to which applications should be made. (If there is any doubt as to where to send the request, make contact with the organisation first and clarify. Most organisations are very familiar with their obligations under the Acts and will be able to provide the necessary information.) Applicants should keep a copy of the request letter and the date it was sent.

Does an email count as a written request?

- Yes, email is also a valid form when making a Section 4 request. Again, requesters should keep a copy of the email and the date it was sent.

How long does it take?

- Under the Acts, an organisation has **40 days** from the date it receives a valid Section 4 request to supply the requester with a copy of their personal data.

Is there a fee?

- Yes. Organisations are entitled (but not obliged) to charge a fee of €6.35 for Access Requests.

Are there any conditions?

- The personal data sought must be stored electronically or, for paper records, as part of a structured manual filing system which allows the relevant records to be easily identified.

How to make the process faster?

- Requesters should include any details that will help the organisation locate their personal data, e.g. staff ID numbers, the date-range of the data.
- Include a cheque or postal order for €6.35 with the application.

Exemptions and restrictions to the Right of Access

- Section 5 of the Acts set out some exemptions to the right of access. Access to personal data may be refused. These include:
 - Where the data being held is being used by particular bodies such as the Gardaí for the prevention, detection, investigation or prosecution of a crime, or to prevent fraud.
 - If the data is subject to legal professional privilege, meaning the data was created following legal advice from a solicitor, and/or the data was created specifically for an upcoming court case.
 - Where the requester is involved in a claim against an organisation, seeking compensation, and the information reveals details of the organisation's decision process in relation to their claim.
 - If the information is held for statistical purposes, is not shared with any other person or organisation and cannot be identified as belonging to any particular individual.
 - If releasing the data would mean that personal data about another individual would be unfairly disclosed. (Personal data may be released in redacted form so as to protect the other individual's data.)
 - Where the data being sought involves personal opinions that have been expressed by another individual. Specifically, if the opinion was given in confidence, and it

can be proven that the person providing the opinion at the time did so in the expectation of confidence, it does not have to be released. (If the opinion was given as part of regular business communications, does not involve personal opinions, and was given without the expectation of confidentiality, it should be released.)

- In the case of a request for access to personal medical information or social work records, access may be denied if there is reason to believe that releasing the information may cause serious risk to the physical or mental health of the individual. The decision not to release such data must be made after consulting the medical professional(s) most recently responsible for the care/ treatment of the data subject.
- If the personal data requested is impossible to supply, or supplying it would be extremely difficult (disproportionate effort).
- If the personal data has already been supplied in accordance with an access request, but identical requests continue to be made (unless new data has been created since the previous records were released, in which case the updated data must be provided).
- If the data that is requested is not the personal data of the requester, it cannot be released under an access request.

Section 6 - Applying to have personal data corrected, deleted or restricted

Once the right to access has been granted, the requester should be in possession of:

- a copy of their personal data
- the reasons how, why and when their personal data was collected
- details about whether their data has been shared with anyone else (especially without their consent)
- information regarding any errors in the personal data that is held on file

If an individual is unhappy with the way their personal data is being processed, or simply want to have a mistake corrected, they have the following rights under Section 6 of the Data Protection Acts:

The right to change or remove details

- If the personal data held is:
 - factually incorrect
 - was obtained or processed in an unfair way
 - is not kept accurate, complete and up-to-date
 - is being used in a way that is not in keeping with the reason for which it was originally collected

- the data is being stored in an unsafe way, or the storage security measures are inappropriate
- the organisation cannot provide a valid reason to keep it
- the individual can ask to have the data corrected or deleted.

What is the procedure for making an application?

- The individual must write to the organisation and explain why the personal data is incorrect or was unfairly obtained, and make a formal request for correction or deletion.

How long does it take?

- An organisation has **40 days**, from the date it receives the written application, to either comply with the request or explain in writing why it is refusing to do so.

Is there a fee?

- No, there is no fee for this request.

The right to restrict the use of your personal data.

- If the individual believes that their personal data is being used for a purpose of which they were not aware of and did not consent to, they can ask to have the use of their personal data restricted to the main purpose for which they originally supplied it.

What is the procedure for making an application?

- The individual must **write** to the organisation and formally request that they restrict the use of their personal data to the main purpose for which it was originally supplied.

How long does it take?

- An organisation has **40 days**, from the date it receives the written application, to either comply with the request or explain in writing why it is refusing to do so.

Is there a fee?

- No, there is no fee for this request.

Making a complaint to the data protection commissioner (DPC)

When can an individual make a complaint to the DPC?

- If an organisation refuses, ignores or delays dealing with an access request without a legitimate reason, an individual can make a complaint to the Commissioner.
- If an organisation refuses to correct, delete, or otherwise secure an individual's personal data in response to a request, the individual can make a complaint to the Commissioner.

How is a complaint made?

- Complaints to the DPC must be **in writing**. Complaint letters or emails should contain the name of the organisation the complaint is against, the steps they have taken to have their concerns dealt with prior to making the complaint, details of any response(s) the individual received from the organisation, as well as copies of any letters or emails exchanged between the individual and the organisation.

Where should complaints to the DPC be sent?

- Written complaints should be addressed to:
 - The Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois
 - info@dataprotection.ie

Does the DPC award compensation?

- No, the DPC does not award compensation.

How will Access Requests change under GDPR?

The General Data Protection Regulation is a European law with direct effect for all EU member states. It will harmonise data protection law across Europe and comes into effect on May 25th, 2018.

- The rules for dealing with subject access requests will change under the GDPR. In most cases, organisations will not be able to charge for processing an access request, unless they can demonstrate that the cost will be excessive.
- The timescale for processing an access request will also shorten, dropping significantly from the current 40-day period. Requests must be processed as quickly as possible, and cannot take longer than one month.
- Organisations will have some grounds for refusing to grant an access request, such as where a request is deemed manifestly unfounded or excessive. However, organisations will need to have clear refusal policies and procedures in place, and demonstrate why the request meets these criteria.
- Organisations will also need to provide some additional information to people making requests, such as their data retention periods and the right to have inaccurate data corrected.
- The GDPR also includes the right to data portability. In particular, this new right enables an individual to require an organisation to transmit their data to another organisation.

- If an organisation handles a large number of access requests, the impact of the changes could be considerable. The logistical implications of having to deal with requests in a shorter timeframe and provide additional information will need to be factored into future planning for organisations. It could ultimately save the organisation a great deal of administrative cost if they develop systems that allow people to access their data easily online.

Definitions

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

Data Subject: is an individual who is the subject of personal data.

Data Controller: is an organisation or person who (either alone or with others) controls the contents and use of personal data.

Other Frequently Asked Questions

Can an individual access personal data about a child?

Legal guardians can make an access request on behalf of a child. However, once a child is capable of understanding their rights to privacy and data protection, the child should normally decide for themselves whether to request access to data and make the request in their own name.

Where an organisation receives an access request from a legal guardian on behalf of a child who has had direct interaction with that organisation, and/or where that child is capable of understanding their own rights to privacy and data protection, the organisation must take account of the child's rights in deciding how to respond to the access request.

The forthcoming General Data Protection Regulation will require organisations offering online services to children to obtain the consent of a guardian for any child under the age of sixteen years. (This applies to online services where consent is required in order for the child to access that service.) The Irish Government can choose to lower the minimum age threshold to thirteen years.

Can an individual access personal data on someone else's behalf?

In some instances, yes. If, for example, a solicitor is making a request on behalf of their client then the request can be complied with, with signed authorisation from their client. In general, an individual can only make an Access Request for their own personal data.

Can an individual access data about the deceased under the Data Protection Act?

No under the Acts, the right to data privacy only applies to living persons.

CCTV and personal data.

Do Access Rights extend to CCTV footage?

- Yes. CCTV footage which contains an individual's image is personal data. Access to CCTV footage can be sought by making a written application, as outlined in 'Section 4 – Applying for access to a copy of your personal data.'

How to make the process faster?

Include any details that will help the organisation locate the personal data sought. In the case of CCTV footage, provide details of the relevant dates and times.

Are there any additional circumstances that would prevent an individual from seeing or obtaining a copy of their personal data on CCTV?

- Copies of personal data gathered by CCTV can be released in two forms:
 - A video copy of the footage.
 - Still images (photos) taken from the camera. Where still images are provided, they should be at a rate of one photograph per second of video.

If the CCTV footage includes images of other people, their images may be pixilated or otherwise blanked out. Access Requests under the Acts entitle individuals to access their own data; images of other people would be considered third-party data. If everyone who appears in the video or photographs agrees to it, the images can be provided without restriction.

Providing CCTV footage to the Gardaí

- As part of their role in the prevention, detection, investigation and prosecution of crime, Gardaí may legitimately seek access to CCTV footage.

Important

This document is purely for guidance, and does not constitute legal advice or legal analysis. This guide is intended as a starting point only, and organisations may need to seek independent legal advice when reviewing or developing their own processes and procedures or dealing with specific legal issues or queries.

For more detailed guidance, please refer to the 'Accessing Your Personal Information' page on our website, www.dataprotection.ie



Checklist for Individuals



1 Written Request

Find out the appropriate address to send your written request. Never use threatening or offensive language.



2 Your Details

Include your name, address and other information that will identify you, so that the organisation can find your data without delay.



3 Making a Request

State clearly that you are making your request under Section 3 or Section 4 of the Data Protection Acts, 1988/2003.



4 Fast Process

Be specific about the information you want. Dates and names will help the organisation to find the information and speed up the process.



5 How to write a Request

Use straightforward, polite language and avoid writing at length. Keep your request specific, to the point and separate from any other complaints you may have with the organisation.



6 Formats

If you have a preferred format that you would like to receive the information in (e.g. electronically) let the organisation know straight away. As far as possible, they will accommodate you, unless it is impractical or too expensive to do so.



7 Repeat Requests

Don't submit repeat requests while earlier requests are still ongoing. It causes unnecessary delays and confusion.



8 Flexibility

As far as possible, be flexible with your request if the organisation says that it cannot supply all the information in its current format. You may need to narrow the scope of what you are looking for, or provide additional information.



9 Copies and Dates

Keep copies of all your correspondence with the organisation, and note the date when you made your request.



10 Fees & Receipts

If you are asked to pay a fee (€6.35) keep a receipt as proof of payment.



Checklist for Organisations



1 Point of Contact

Have a single point of contact who will coordinate any incoming Access Requests. Any written request from an individual asking for access to their personal data is valid.



2 Timelines

Note the date on which you received the request. That is day one, for the purposes of deciding timelines.



3 Deadlines

You have 21 calendar days to comply with a Section 3 request, and 40 calendar days to comply with a Section 4 request.



4 Proof of I.D

If you are unsure of the identity of the requester, you are entitled to contact them as soon as possible and ask for proof of identification. The 40-day time-limit does not begin until the requester's identity has been confirmed, but you must not use this facility to unduly delay the process.



5 Need More Information

If you need more information to identify what data the requester is looking for, contact them without delay. This is included in the 40-day time limit.



6 Fees & Charges

You can charge a fee (€6.35) for Section 4 requests. Notify the requester and compile the information they seek. You can withhold the information until the €6.35 is paid, but you must be ready to hand over the data immediately the fee is received.



7 Amendments

You must not make any changes to, or destroy, the individual's records once you have received a Section 3 or Section 4 request, even if the information is incorrect or potentially embarrassing. Scheduled routine amendments (such as calculating interest) can continue after a request has been received.



8 Your Obligations

If the data contains information about other people, you are obliged to redact or withhold that information, unless (i) the other parties give their consent or (ii) the information was supplied in an official capacity in the course of work.



9 Unfamiliar Terms or Codes

If the information contains codes or terms that would be unfamiliar to the requester, you must provide an explanation.



10 Data Forms

You must provide a copy of the data in a form that is accessible to the requester. Prepare a detailed list of the data that you will be releasing, as this is of assistance if disputes arise over records that are incomplete or withheld.