An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Rights of Individuals under the General Data Protection Regulation

2018

Contents

Important: This document is purely for guidance, and does not constitute legal advice or legal analysis.

Up to date as of 28.02.2018

Introduction

Data protection is a fundamental right set out in Article 8 of the EU Charter of Fundamental Rights

> *1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *3. Compliance with these rules shall be subject to control by an independent authority.*

The General Data Protection Regulation ('GDPR') is applicable from 25th May 2018 and is designed to give individuals more control over their personal data. The key principles under the GDPR are:

- Lawfulness, fairness and transparency;
- Purpose Limitation;
- Data minimisation;
- Accuracy;
- Storage Limitation;
- Integrity and confidentiality and
- Accountability.

This document is intended to guide you through your rights, as data subjects, under the GDPR.

Glossary

The following terms used throughout this guide have specific legal meanings under the GDPR. In order to understand your rights fully, please read the following glossary of key terms.

Personal data

The term "personal data" means any information relating to a living person who is identified or identifiable (such a person is referred to as a "data subject").

A person is identifiable if they can be identified directly or indirectly using an "identifier". The GDPR gives examples of identifiers, including names, identification numbers, and location data. A person may also be identifiable by reference to factors which are specific to their identity, such as physical, genetic or cultural factors.

Processing

The term "processing" refers to any operation or set of operations performed on personal data. Processing includes storing, collecting, retrieving, using, combining, erasing and destroying personal data, and can involve automated or manual operations.

Data Protection Commission

The "Data Protection Commission" ('Commission') is the body which will be established under Data Protection Act 2018 and which will replace the Data Protection Commissioner's office. The Commission will be a supervisory authority i.e. an independent public authority, established under the GDPR, with responsibility for monitoring the application of the GDPR.

Data Controller

A "data controller" refers to a person, company, or other body which determines the purposes and means of processing of personal data.

Data Processor

A "data processor" refers to a person, company, or other body which processes personal data on behalf of a data controller.

Consent

Some types of processing are carried out on the basis that you have given your consent. Under the GDPR, consent to processing must be freely given, specific, and informed. You cannot be forced to give your consent, you must be told what purpose(s) your data will be used for and you should show your consent through a 'statement or as a clear affirmative action' (e.g. ticking a box).

Consent is not the only lawful basis on which your personal data can be processed. Article 6 of the GDPR sets out a complete list of lawful purposes for processing personal data (please see footnote on page 5 of this guide).

Profiling

Profiling is any kind of automated processing of personal data that involves analysing or predicting your behavior, habits or interests.

Special categories of personal data

Certain types of sensitive personal data are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as “special categories” of personal data. The special categories are: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person’s sex life or sexual orientation. Processing of these special categories is prohibited, except in limited circumstances set out in Article 9.

What rights do you have?

1. The right to be informed (Article 13 & 14 of the GDPR)

What information must a data controller provide where the personal data is collected from you?

Where the personal data is collected from you, the data controller must provide you with the following information:

1. Identity and contact details of the data controller (and where applicable, the controller's representative);
2. Contact details of the Data Protection Officer (person with responsibility for data protection matters within the organisation);
3. Purpose(s) of the processing and the lawful basis for the processing;
4. Where processing is based on the legitimate interests of the controller or a third party, the legitimate interests of the controller[1];
5. Any other recipient(s) of the personal data;
6. Where applicable, details of any intended transfers to a third country (non-EU member state) or international organisation and details of adequacy decisions and safeguards;
7. The retention period (how long an organisation holds onto data) or, if that is not possible, the criteria used to determine the retention period;
8. The existence of the following rights –
    - Right of access
    - Right to rectification
    - Right to erasure
    - Right to restrict processing
    - Right to data portability
    - Right to object –

    and to request these from the data controller.
9. Where processing is based on consent, the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
10. The right to lodge a complaint with a supervisory authority;
11. Whether the provision of personal data is a statutory or contractual requirement, necessary to enter into a contract, an obligation, and the possible consequences of failing to provide the personal data;

[1] **Lawful basis for processing personal data**: In order to process personal data, organisations must have a lawful basis to do so. The lawful grounds for processing personal data are set out in Article 6 of the GDPR. These are: with the consent of the individual; in the performance of a contract; in compliance with a legal obligation; where necessary to protect the vital interests of a person; where necessary for the performance of a task carried out in the public interest; or in the legitimate interests of company/organisation (except where those interests are overridden by the interests or rights and freedoms of the data subject.

12. The existence of any automated decision making processes that will be applied to the data, including profiling, and meaningful information about how decisions are made, the significance and the consequences of processing.

When should this information be provided to you?

- At the time your personal data is collected from you.

How will this information be provided to you?

- Clear guidance on this process can be found in the section 'How will the information be provided?' (page 12 of this guide).

What happens when the data controller intends to process your personal data for a purpose other than that for which it was originally collected?

Where the controller intends to process your personal data for another purpose (other than the purpose for which the data was originally collected):

- The controller must provide you, prior to that other processing, with any further relevant information as per 1 – 12 above.

Are there any circumstances in which these requirements will not apply?

The above requirements will not apply:

- Where you already have the above information.

What information must a data controller provide where the personal data has not been obtained from you?

Where the personal data has not been obtained from you, the data controller must provide you with:

1. The information at 1 - 10 & 12 above;
2. Information on the types of personal data they hold about you;
3. Information on how they obtained the personal data and whether it came from publicly accessible sources.

When should this information be provided to you?

- Within a reasonable period of having obtained the data and, at the latest, within one month;
- If the data is used to communicate with you, at the latest, when the first communication takes place;
- If it is expected that your personal data will be disclosed to another recipient, when your personal data is first disclosed.

How will this information be provided to you?

- Clear guidance on this process can be found in the section 'How will the information be provided?' (page 12 of this guide).

What happens when the data controller intends to process your personal data for a purpose other than that for which it was originally collected?

Where the controller intends to process your personal data for another purpose (other than the purpose for which the data was originally collected):

- The controller must provide you, prior to that other processing, with any further relevant information.

Are there any circumstances in which these requirements will not apply?

The above requirements will not apply:

- Where you already have the above information;
- Where the provision of such information is impossible or would involve a disproportionate effort;
- Where obtaining the information or disclosure is a legal obligation and
- Where the personal data must remain confidential due to an obligation of professional secrecy regulated by law.

This right will typically be fulfilled through a 'Privacy Notice'.

2. The right to access information (Article 15 of the GDPR):

You have the right to obtain the following, from the data controller:

1. Confirmation of whether or not personal data concerning you is being processed;
2. Where personal data concerning you is being processed, a copy of your personal information;
3. Where personal data concerning you is being processed, other additional information as follows:
    1. Purpose(s) of the processing;
    2. Categories of personal data;
    3. Any recipient(s) of the personal data to whom the personal data has or will be disclosed, in particular recipients in third countries or international organisations and information about appropriate safeguards;
    4. The retention period or, if that is not possible, the criteria used to determine the retention period;
    5. The existence of the following rights –
        i. Right to rectification
        ii. Right to erasure
        iii. Right to restrict processing
        iv. Right to object –

        and to request these from the controller.

    6. The right to lodge a complaint with a supervisory authority (in Ireland this is the Data Protection Commissioner, whose contact details are on page 14 of this guide);

7. Where personal data is not collected from the data subject, any available information as to their source;
8. The existence of automated decision making, including profiling and meaningful information about how decisions are made, the significance and the consequences of processing.

The right to the information above must not adversely affect the rights and freedoms of others.

Can the data controller charge a fee to provide a copy of the information?
No, the data controller must provide a copy of the information:

- For free;
- However, if any further copies are requested by the data subject, the controller may charge a reasonable fee.

What happens if you make the access request by electronic means?
- The information must be provided in electronic form, unless otherwise requested by you.

3. The right to rectification (Articles 16 & 19 of the GDPR)

If your personal data is inaccurate, you have the right to have the data rectified, by the controller, without undue delay.

If your personal data is incomplete, you have the right to have data completed, including by means of providing supplementary information.

4. The right to erasure (Articles 17 & 19 of the GDPR)

This is also known as the '*right to be forgotten*'.

You have the right to have your data erased, without undue delay, by the data controller, if one of the following grounds applies:

1. Where your personal data is no longer necessary in relation to the purpose for which it was collected or processed;
2. Where you withdraw your consent to the processing and there is no other lawful basis for processing the data;
3. Where you object to the processing and there is no overriding legitimate grounds for continuing the processing (See point 6 below).
4. Where you object to the processing and your personal data is being processed for direct marketing purposes (See point 6 below);
5. Where your personal data has been unlawfully processed;
6. Where your personal data have to be erased in order to comply with a legal obligation;
7. Where your personal data has been collected in relation to the offer of information society services to a child.

What happens when the data controller made your personal data public and is obliged to erase the data?

Where the data controller has made your personal data public and, on the basis of one of the above grounds, is obliged to erase the data:

- The data controller must communicate any rectification or erasure of your personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort.
- If you request information on recipients of your personal data, the data controller must inform you about the recipients.
- The data controller shall take reasonable steps to inform other controllers, who are processing your personal data, that you have requested the erasure by them of any links to or copies of your data.
  Reasonable steps means taking account of available technology and the cost of implementation including technical measures.

Are there circumstances in which the right to be forgotten will not apply?

Yes, the right to be forgotten will not apply where processing is necessary for:

- Exercising the right of freedom of expression and information;
- Compliance with a legal obligation, the performance of a task carried out in the public interest or in the exercise of official authority;
- Reasons of public interest in the area of public health (See Article 9(2)(h) & (i) and Article 9(3), GDPR)
- Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;
- Establishment, exercise or defence of legal claims.

5. The right to data portability (Article 20 of the GDPR)

In some circumstances, you may be entitled to obtain your personal data from a data controller in a format that makes it easier to reuse your information in another context, and to transmit this data to another data controller of your choosing without hindrance. This is referred to as the right to data portability.

When does the right to data portability arise?

This right only applies where processing of personal data (supplied by the data subject) is carried out by automated means, and where you have either consented to processing, or where processing is conducted on the basis of a contract between you and the data controller.

This right only applies to the extent that it does not affect the rights and freedoms of others.

When this right applies, how must data controllers provide and transmit data?

Where this right applies, data controllers must provide and transmit personal data in structured, commonly used and machine readable form. Data is structured and machine readable if it can be easily be processed by a computer.

Under this right, you can ask a data controller to transmit your data to another data controller, if such transmission is technically feasible.

6. The right to object to processing of personal data (Article 21 of the GDPR)

When do you have a right to object?

You have the right to object to certain types of processing of your personal data where this processing is carried out in connection with tasks in the public interest, or under official authority, or in the legitimate interests of others.

You have a stronger right to object to processing of your personal data where the processing relates to direct marketing. Where a data controller is using your personal data for the purpose of marketing something directly to you, or profiling you for direct marketing purposes, you can object at any time, and the data controller must stop processing as soon as they receive your objection.

You may also object to processing of your personal data for research purposes, unless the processing is necessary for the performance of a task carried out in the public interest.

How do you object to processing?

In order to object to processing, you must contact the data controller and state the grounds for your objection. These grounds must relate to your particular situation. Where you have made a valid objection, the data controller must cease processing your personal data, unless the data controller can provide compelling legitimate reasons to continue processing your data. Data controllers can also lawfully continue to process your personal data if it is necessary for certain types of legal claims.

What obligations do data controllers have in relation to this right?

Where the right to object applies, data controllers are obliged to notify you of this at the time of their first communication with you. Where processing is carried out online, data controllers must offer an online method to object.

7. The right of restriction (Article 18 of the GDPR)

You have a limited right of restriction of processing of your personal data by a data controller. Where processing of your data is restricted, it can be stored by the data controller, but most other processing actions, such as deletion, will require your permission.

How does this right apply?

This right applies in four ways. The first two types of restriction of processing apply where you have objected to processing of your data under Article 21, or where you have contested the accuracy of your data. In these cases, the restriction applies until the data controller has determined the accuracy of the data, or the outcome of your objection.

The third situation in which you can request restriction relates to processing which is unlawful. In these cases, if you do not want the data controller to delete your information, you can request restriction of the personal data instead.

The fourth type of restriction of processing applies where you require data for the purpose of a legal claim. In this case, you can request restriction even where the data controller no longer needs the data.

When you have obtained restriction of processing, what obligations does the data controller have?

Where you have obtained restriction of processing of your data, the data controller must inform you before lifting the restriction.

8. Your rights in relation to automated decision making, including profiling (Article 22 of the GDPR)

You have the right to not to be subject to a decision based solely on automated processing. Processing is "automated" where it is carried out without human intervention and where it produces legal effects or significantly affects you.

Automated processing includes profiling.

In respect of personal data, when is automated processing permitted?

Automated processing is permitted only with your express consent, when necessary for the performance of a contract or when authorised by Union or Member State law. Where one of these exceptions applies, suitable measures must be in place to safeguard your rights, freedoms and legitimate interests. This may include the right to obtain human intervention on the controller's part, the right to present your point of view and the right to challenge the decision.

In respect of special category personal data ('sensitive'), when is automated processing permitted?

Where automated processing relates to the special categories of personal data (outlined in the glossary above), processing is only lawful where you have given your express consent to the processing, or where it is necessary for reasons of substantial public interest.

Matters which apply to all the rights detailed above (Article 12 of the GDPR)

Restrictions on exercising rights:

The GDPR (Article 23) allows all the rights detailed in this document –

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object;
8. Rights in relation to automated decision making and profiling –

- to be restricted by national law in certain circumstances for example, the prevention and detection crime. The Data Protection Bill 2018 is currently progressing through the Houses of the Oireachtas and currently provides for certain restrictions on the exercise of data subject rights. The Bill (once enacted) will set out clearly the circumstances in which the rights set out in this document will be restricted.

How will the information be provided?

When you exercise your rights under the General Data Protection Regulation, the information provided to you must be:

- Provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, particularly for any information addressed to a child.
- The information must be provided in writing, or by other means, including, where appropriate, by electronic means.
- Where the data subject makes the request by electronic form means, where possible, the information must be provided by electronic means, unless otherwise requested by you.
- When requested by you, the information may be provided orally, provided that your identity is proven by other means.
- Except in the cases where your rights are restricted, a data controller cannot refuse to act on your request to exercise your rights unless the controller demonstrates that it is not in a position to identify you.
- Where a data controller has reasonable doubts about your identity, the data controller may request the provision of additional information necessary to confirm your identity. This is only

applicable in respect of the rights of access, to rectification, erasure, restrict processing, data portability, to object and in relation to automated decision making and profiling.

What are the timeframes for dealing with requests to exercise my rights?

When a request to exercise your rights is made, a data controller must:

- Provide information on action taken without undue delay;
- In any event, within 1 month of receipt of the request;
- The 1 month period may be extended by 2 further months, where necessary, taking into account the complexity and number of requests, where necessary.
    - In this case, the data controller shall inform you of any extension within 1 month of receipt of the request and the reasons for the delay.
- If the controller does not take action on foot of your request, the data controller must inform you without delay and, at the latest, within 1 month of receipt of your request, of:
    - The reasons for not taking action;
    - The possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

What are the charges?

Your requests will be dealt with free of charge.

However, where requests from a data subject are considered 'manifestly unfounded or excessive' (for example where an individual continues to make unnecessary repeat requests or the problems associated with identifying one individual from a collection of data are too great) the data controller may:

1. Charge a reasonable fee, taking into account the administrative costs of providing the information/ taking the action requested; or
2. Refuse to act on your request.

In cases where this is used as a reason to refuse an access request or to charge a fee, it is up to the organisation to prove why they believe the request is manifestly unfounded or excessive.

Making a complaint to the Data Protection Commission

Under Article 77 of the GDPR, you have the right to lodge a complaint with the Data Protection Commission if you consider that processing of your personal data is contrary to the GDPR.

Under Article 78 of the GDPR, you have a right to an effective judicial remedy where the Data Protection Commission does not handle your complaint, or does not inform you within three months on the progress or outcome of your complaint.

Under Article 80, you may authorise certain third parties to make a complaint on your behalf.

From 25th May 2018, there will be a new mechanism for lodging complaints to the Data Protection Commission. Complaints should be submitted via the **online form** available at www.dataprotection.ie.

In the meantime, complaints to the Commission can be made in writing and addressed to:

info@dataprotection.ie
or
The Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois

The Data Protection Commissioner also operates a helpdesk function, which is contactable at:

0761104 800
or
LoCall 1890 252231