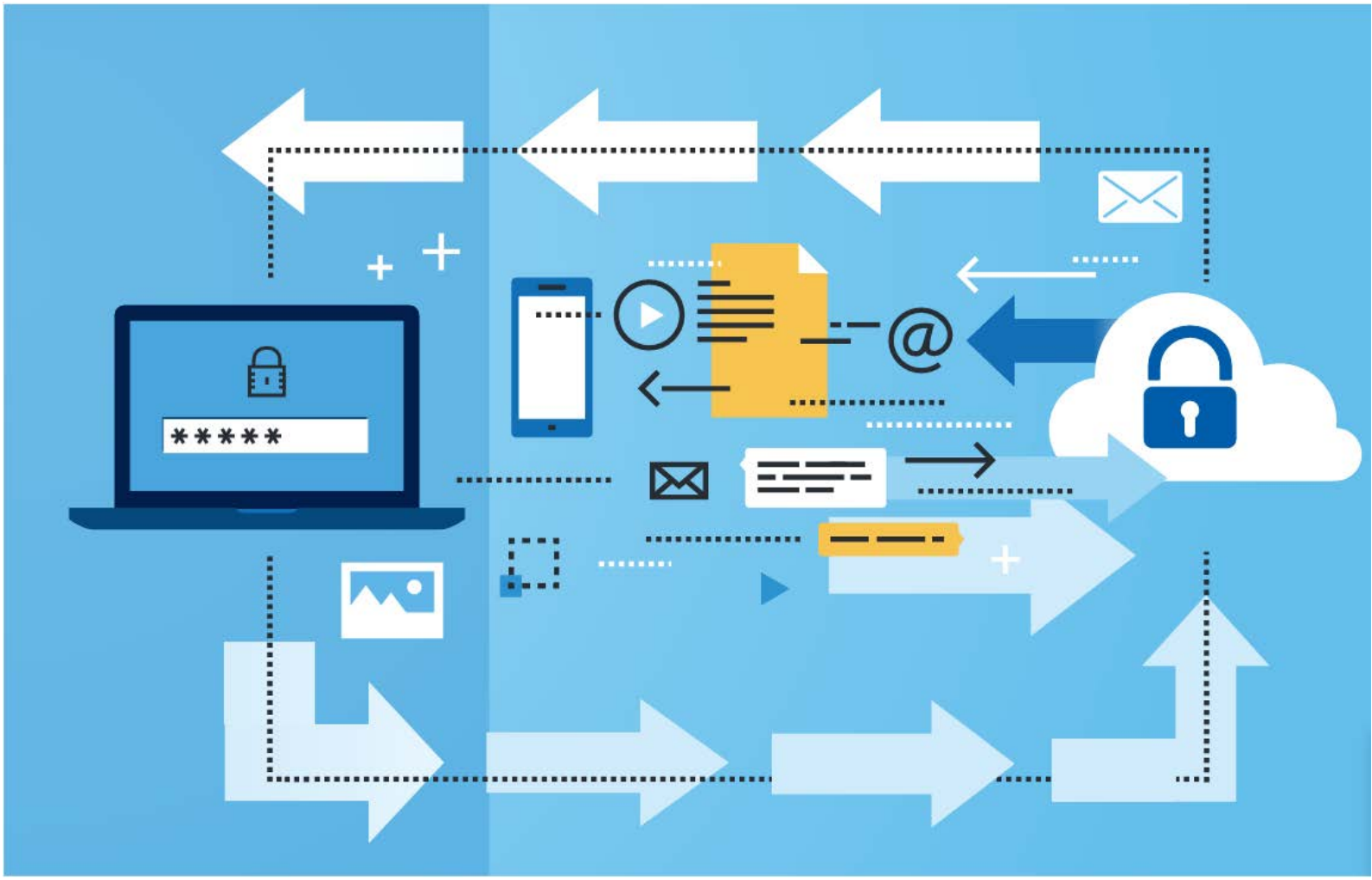
Data Protection Rights for NGOs

November 2022



CONTENTS

Section **PAGE**

Introduction

Data protection law is concerned with the protection of the personal data of living individuals. In Ireland, data protection rights and obligations are governed primarily by the General Data Protection Regulation and the Data Protection Act 2018 ("**Data Protection Law**"). This guide is intended to provide an overview of Data Protection Law and its application to the charity/not-for-profit sector. It is divided into two sections; the first focuses on data protection rights from the perspective of individuals and the second outlines data protection obligations for organisations.

The following are key data protection terms and concepts.

1. What is personal data?

Personal data is any information which relates to an identified or identifiable individual, which is defined as anyone who can be directly or indirectly identified from the data. It is interpreted broadly and covers a much broader range of information (e.g. beyond an individual's name, address, contact details, etc.) than some people might expect.

2. Who is a controller?

A controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing personal data (e.g. an employer in relation to their employee's data, a GP in relation to their patient's data, etc.).

3. Who is a processor?

A processor is a natural or legal person, public authority, agency or other body that processes personal data on behalf of a controller (e.g. a payroll service provider that manages payments to employees on behalf of an employer, or a call centre taking calls on behalf of a charity).

4. What does 'process' mean?

In this context, 'process' essentially means anything that is done to or with a person's data. 'Processing' includes collecting, recording, keeping, disclosing, publishing, using or deleting data. Data processing occurs when one's data is collected and translated into usable information.

5. Are there any exemptions to when Data Protection Law will apply to processing of personal data?

The GDPR does not apply to an organisation which does not operate within the EU, where an organisation does not process personal data, or where an individual processes personal data in the course of a *purely* personal or household activity (the '**household exemption**').

This household exemption relates to the processing of personal data which has no connection to a professional or commercial activity. For example, this exemption applies to social networking by an individual where the activities are purely personal. However, the GDPR would still apply to an organisation that processes personal data in connection with activity on a social network. The household exemption also applies to an individual keeping an address book and personal correspondence.

When processing takes place for law enforcement purposes, such as by the Gardaí, the GDPR does not apply. Instead, the EU Law Enforcement Directive ('**LED**') applies, which was implemented into Irish law by Part 5 of the Data Protection Act 2018.

6. Who is a data subject?

Any living individual who is the subject of personal data.

7. What are special categories of personal data?

Under Data Protection Law, special categories of personal data are subject to additional protection. These special categories are:

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- Genetic data and biometric data processed for the purpose of uniquely identifying a natural person;
- Data concerning health; and
- Data concerning an individual's sex life or sexual orientation.

Guidance

This document is for general guidance only and is not intended to be, and should not be relied upon as a substitute for, legal advice. Reference is made throughout the guide to the need for proper internal policies regarding an organisation's approach to data protection. As a member of PILA you can access the Pro Bono Referral Scheme where your organisation can access relevant legal expertise and support with this.

Further details regarding Data Protection Law and best practice are available on the website of the Data Protection Commission - www.dataprotection.ie and the website of the European Data Protection Board - www.edpb.europa.eu.

1. Data Protection Rights for Individuals

Introduction

This section of the guide provides an outline of the rights that apply to you, as an individual, in respect of your personal data and the responsibilities of organisations who hold and process your personal data. It is important to know that Data Protection Law only applies to data relating to living individuals and does not apply to data relating to deceased persons. In addition, the rules do not apply to data about companies or any other legal entities. However, information in relation to one-person companies may constitute personal data where it relates to that person. The rules also apply to all personal data relating to natural persons in the course of a professional activity, such as the employees of a company/organisation, business email addresses like 'forename.surname@company.eu' or employees' business telephone numbers.

Personal data relating to an individual is likely to be held by many different organisations, such as government bodies, public authorities, healthcare providers, educational institutions, banks, insurance companies, communication service providers, retailers, etc. You have rights as a data subject in relation to any personal data relating to you that is held by any such organisation.

The Data Protection Commission of Ireland (the "DPC") is responsible for monitoring and enforcing compliance with Data Protection Law, including ensuring that your rights as a data subject are respected.

As a data subject, you have a range of rights in respect of your personal data which apply where a controller holds your personal data in any form. In general, another individual or organisation can assist you in exercising and enforcing your rights as a data subject, as long as they are acting with your consent and this can be demonstrated to the relevant controller (e.g. by a letter signed by you confirming that your representative is acting on your behalf).

Rights of a Data Subject

As a data subject, you have the following rights under Data Protection Law:

1. The right to be informed

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

- The identity and contact details of the controller (and where applicable, the controller's representative);
- Contact details of the organisation's Data Protection Officer, where applicable;
- Information on the purpose and lawful basis for the processing;
- Where processing is based on the legitimate interests of the controller or a third party, the legitimate interests relied upon;
- Any other recipient(s) of the personal data;
- Where applicable, details of any intended transfers of your data outside the European Economic Area ("EEA") as well as details of any relevant adequacy decisions or safeguards;
- The retention period (how long the controller holds onto data) or, if that is not possible, the criteria used to determine the retention period;
- The existence of the following rights (discussed below) - o Right of access o Right to rectification o Right to erasure o Right to restrict processing o Right to data portability o Right to object;
- 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;
- The right to lodge a complaint with a supervisory authority;
- Whether the provision of personal data is a statutory or contractual requirement and the possible consequences of failing to provide the personal data; and
- Whether the controller plans on further processing the personal data for a purpose other than the original one.

The controller must provide the above information to you at the time of collecting your data. Often, this information will be included in the controller's data protection/privacy notice.

Where personal data relating to you is collected indirectly by a controller (e.g. from another organisation), the controller is required to provide you with similar details, except where the provision of these details is impossible or would involve a disproportionate effort on the part of the controller.

There are limited circumstances in which the above requirements will not apply. For example, a controller does not have to provide an individual with the above information regarding the collection and use of personal data relating to that individual where withholding it is necessary and proportionate in connection with a criminal investigation or prosecution, or in relation to any legal claim.

2. The right of access

You have the right to submit an access request to a controller at any time, seeking the following information:

- Confirmation of whether or not your personal data is being processed;
- Where your personal data is being processed, a copy of that personal data as well as information in relation to:
    - The purpose of the processing
    - The categories of personal data held
    - Any recipients of the personal data including recipients in countries outside the EEA
    - The retention period, or the criteria used to determine the retention period
    - The existence of your rights as data subject;
- Where personal data is not collected directly from you, any available information as to the source of the data; and
- The existence of automated decision making, including profiling and meaningful information about how decisions are made, the significance and the consequences of processing.

The controller must respond to your access request without undue delay and within one month of receiving the request. If your request is complex or relates to a large volume of material, this deadline can be extended by two months. In this case, the controller must contact you within one month of receiving your access request, providing a reason for the delay.

The controller cannot charge a fee for responding to your access request. The controller can, however, charge a reasonable fee for any additional copies of the data requested. The controller must provide your personal data to you in a form that is concise, transparent and understandable.

Case Study

A complainant was dissatisfied when his request for access to a copy of information kept by a controller in electronic and in manual form was refused by the controller, a County Council. The County Council informed the complainant that the requested files were available online or for viewing at the County Council's premises. The complainant and the County Council disagreed as to whether the files made available at the County Council's premises constituted all of the personal data concerning the complainant which the County Council held. The County Council sought to distinguish between personal data relating to the publicly available planning files, which was supplied to the complainant at a public viewing, and personal data created following the refusal of the complainant's planning application, which the County Council considered to be outside the scope of the access request. While the complainant mentioned two specific planning applications, the access request overall sought access to "any information you keep about me electronically or in manual form." The DPC held that the County Council erred in its data protection obligations when it failed to supply the complainant with a complete copy of the complainant's personal data in response to the access request within the statutory period. The GDPR places an onus on the County Council, as controller, to provide information on the action taken under such a request without undue delay and in any event within one month of receipt of the request. The case study is available here: https://dataprotection.ie/en/dpcguidance/dpc-case-studies#202001.

3. The right to rectification

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

As a data subject, you have the 'right to be forgotten'. This means that you have the right to have your data erased by the controller, without undue delay, if one of the following grounds applies:

- Your personal data is no longer necessary in relation to the purpose for which it was collected or processed;
- You withdraw your consent to the processing and there is no other lawful basis for processing the data;
- You object to the processing and there is no overriding legitimate grounds for continuing the processing;
- You object to the processing in circumstances where your personal data is being processed for direct marketing purposes;
- Your personal data has been unlawfully processed;
- Your personal data has been erased in order to comply with a legal obligation; or
- Your personal data has been collected in relation to the offer of information society services to a child.

Your right to erasure can be denied by the controller where the 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;
- Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
- Establishment, exercise or defence of legal claims.

5. The right to data portability

In some circumstances, you have the right to request a copy of your data from the controller in a structured, commonly used and machine readable format and to request the controller to transfer your data to another controller. This right only arises where the processing of your data is carried out by automated means and where the processing is carried out on the basis of your consent, or on the basis of a contact between you and the controller.

6. The right to object to processing

You have the right to object to the processing of your data where the processing is carried out in connection with tasks in the public interest, under official authority or for the purposes of legitimate interests pursued by others. For example, a company might set up CCTV systems to monitor the entrance to their premises for security purposes, or for other purposes (such as monitoring attendance) and do so by reference to legitimate interests it is pursuing. An individual would have the right to object to the processing of his or her data through the video surveillance systems, where the company is doing so for the purposes of 'legitimate interests'.

The grounds of objection can be based on your particular situation and the controller can only further process your data despite your objection if they have shown a compelling reason to do so, which overrides your interests. For example, employers may process personal data relating to their employees in relation to dealing with a grievance based on this being necessary for the purpose of investigating the employee's grievance, a legitimate interest,(such as?) pursued by the employer.

An employee involved in the grievance might object to the processing of their personal data on this legitimate interest basis. However, the employer may be able to justify continuing to process that individual's personal data in these circumstances, despite their objection, since the employer would be doing so for compelling legitimate grounds. This right also covers a right to object to your data being processed for direct marketing purposes and for research purposes, unless the processing is necessary for the performance of a task carried out in the public interest.

7. The right to restrict processing

In some circumstances, you have the right to limit the way controllers use your personal data, instead of requesting erasure. This right is not absolute and is only exercisable where:

- The controller is responding to a request to rectify your data;
- You have objected to the processing of your data and the controller is verifying the request;
- The processing is unlawful but you do not want the controller to erase the data; or
- The controller no longer needs the personal data for the purposes of the processing, but you require them to keep it for a legal claim in which you are involved.

Once the request to restrict your data is received, the controller will be permitted to store the data, while most other processing actions will require your permission.

8. Rights in relation to automated decision making

You have the right not to be subject to decisions based solely on automated means, where that decision produces legal effects or significantly affects you. This type of processing may be permitted in exceptional circumstances, however, where it is necessary for the performance of a contract, authorised by Union or Member State law or carried out on your express consent. Where one of these exceptions applies, suitable measures must be in place to safeguard your rights, such as the right to obtain human intervention in the processing, the right to present your point of view and the right to challenge the decision.

Where the processing relates to special categories of personal data, the use of automated decision making will only be lawful where you have given your express consent to the processing, or where it is necessary for reasons of substantial public interest.

Direct Marketing

In addition to the General Data Protection Regulation and the Data Protection Act 2018, the ePrivacy Regulations 2011 (the "**e-Privacy Regulations**") set out further rules that apply to certain types of data processing, including electronic direct marketing (marketing conducted by phone, fax, text message, and email). The general rule (subject to limited exceptions) is that controllers require your clear, affirmative consent, in order to be entitled to send you electronic direct marketing (for example by providing an opt-in mechanism). The controller cannot use an opt-out mechanism, or pre-ticked boxes, in seeking your consent to direct marketing.

Controllers do not need affirmative consent in order to send electronic direct marketing messages to you if you are an existing customer, provided the following conditions are met:

- The product or service being marketed is the organisation's own product or service;
- The product or service being marketed is of a kind similar to that supplied to you in the context of the original transaction;
- You must be given the opportunity to object to the use of your details at the time those details are collected, as well as each time the organisation sends an electronic direct marketing message to you; and
- The initial direct marketing communication must be sent within 12 months of the date of the original transaction.

Where the controller relies on your consent in sending direct marketing messages to you, you can withdraw that consent at any point. As noted above, you also have the right to object to the processing of your data for direct marketing purposes at any point.

The EU intends to introduce an e-Privacy Regulation which will give data subjects additional rights in this area. Once this Regulation is adopted and brought into force, it will supersede the current ePrivacy Regulations. The finalisation of this Regulation has taken much longer than was intended. At one time it was intended that it would be adopted shortly after the GDPR became applicable in 2018, however it remains a work in progress in the EU legislative process. At the time of writing this guide, it seems unlikely to become applicable before 2025 at the earliest.

Time Limits

When you make a request to exercise your rights, the controller must act on the request without undue delay and in any event within one month of receipt of the request. This one month period may be extended by a further two months where the request is complex or where it relates to a large volume of material. In this case, the controller must inform you of the extension of time within one month of receiving your request, providing reasons for the delay. If the controller chooses not to act on your request, it must inform you of this decision without delay and in any event within one month of receipt of your request. In this case, the controller must inform you of its reasons for not acting on your request and the possibility of lodging a complaint with the DPC and seeking a judicial remedy.

Making a Complaint

If a controller fails or refuses to give effect to any of your rights as a data subject, or if you have not received a satisfactory response within the appropriate time period, then you can make a complaint in writing to the Data Protection Commission (the "**DPC**"). Complaints can be made via the DPC's website: https://forms.dataprotection.ie/contact. Alternatively, you can make written submissions to:

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2

The DPC also has offices at:

Canal House, Station Road
Portarlington, Co. Laois
R32 AP23

It is important to note that the Data Protection Commission does not have a public counter and therefore is not in a position to provide face-to-face meetings. If you are not in a position to engage with the office by the above mentioned means, however, please contact the DPC's Accessibility Officer at *DPCAccessibilityOfficer@dataprotection.ie*

In your submission, you should include the following information:

- Details of the specific data protection issue you are raising;
- Signed authority from you, where a solicitor/representative has made the contact;
- Documentary evidence to support the allegation being made; and
- A copy of relevant correspondence exchanged with the controller on the matter.

Where the complaint relates to direct marketing, you should also include the following information:

- The email address/phone number/fax number to which the marketing material was sent;
- Confirmation of who your phone service provider is;
- Details of where the marketing issued from (the name of the controller as well as the email address/phone number it issued from);
- A copy of the marketing material received; and

- Details of any attempts made by you to opt-out of receiving marketing material or calls from the controller.

For more information on submitting a complaint, please consult the DPC website: https://www.dataprotection.ie/en/individuals/exercising-your-rights/raising-concernevidence-may-be-required-dpc.

Freedom of Information

Although this guide is intended to focus on Data Protection Law only, it is worth mentioning the freedom of information regime since it overlaps with Data Protection Law in some areas.

The Freedom of Information Act 2014 (the "FOI Act") applies to public bodies, except those which are listed as exempt under the FOI Act. The aim of the FOI Act is to ensure that the relevant FOI bodies are open and transparent by ensuring that their records should be available for access to all members of the public. There are a number of exemptions which apply to the records and information that may be released under the FOI Act. For example, certain confidential, commercially sensitive or personal information may be withheld, except where the public interest in the information being released would outweigh the public interest in such information being withheld. The Office of the Information
Commission oversees the operation of the FOI Act and will review, on application, decisions made by FOI bodies under the FOI Act.

An individual has a right to seek access to any record held by a FOI body, to obtain reasons for a decision or act of a FOI body affecting him/her, and to have any personal information held by a FOI body in relation to that individual amended where it is incomplete, incorrect or misleading. Where the FOI Act applies, it provides for rights of access to personal information and rectification which are similar to the rights of access and rectification provided for under Data Protection Law.

You can seek access to records and/or personal information relating to you by writing to the FOI body, addressing the request to the 'Freedom of Information Unit/Officer', and including the following information:

- State that the request is made under the FOI Act;
- Provide sufficient details in relation to the information concerned in order for the
- FOI body to know what you are looking for; and
- If you require access to be given in a particular form or manner, specify the form or manner of access.

A FOI request must be acknowledged within 2 weeks of receipt and the FOI body must then decide to grant, refuse or accept the request in full or in part, generally not later than 4 weeks after the receipt of the request.

It is possible for the timeframe for making the decision to be extended in some circumstances (e.g. it can be extended by up to a further 7 weeks where it is necessary to consult with affected third parties, or by up to a further 4 weeks where the request relates to such a large number of records that dealing with it within 4 weeks would not be possible). The FOI body must also inform the requester of any fees that will be payable (however no fees may be charged for providing an individual with personal information relating to themselves). If you do not receive a response within the 4week period, then under the FOI Act, your request will be deemed to have been refused.

If you are unhappy with a decision issued by a FOI body, you may apply for an internal review within the FOI body concerned. A request for internal review must be made within 4 weeks of the original decision, and a response must issue from the FOI body within 3 weeks of receipt of the request. If you are still unhappy with this response, you can apply for a review of the decision by the Information Commissioner. In this instance, you must make a request for review of the decision in writing within 6 months of notification of the decision. Applications to the Information Commissioner for review can be made online using the only application form available at https://www.oic.ie/apply-for-a-review/start-application/, by email, by post or by hand-delivering the application form to:

18 Lower Leeson Street
Dublin 2
D02 HE97

The decision which issues from the Commissioner's review is legally binding but can be appealed to the High Court on a point of law. An appeal to the High Court must be brought within 4 weeks from the date of the decision. Legal advice should be sought in advance of considering an appeal before the High Court.

Checklist of information to include in a letter seeking access to information from a FOI body:

- Refer to the fact that you are making a request under Freedom of Information Act 2014;
- Specify the format that you wish to receive the documents in (e.g. digital or paper form);
- Make the request as specific as possible (e.g. list out what you want to receive and the relevant time period for the particular records); and
- Request that the letter is acknowledged, and refer to the fact that the FOI body is required, under Section 13(1) of the FOI Act, to notify the sender of its decision in relation to the request within 4 weeks of its receipt.

2. Data Protection for Organisations

Introduction

An organisation that collects, stores or processes any personal data relating to living people (e.g. customers, employees, donors, volunteers, clients etc.) is a controller, a processor, or both and has obligations in relation to that personal data under Data Protection Law.

To determine whether your organisation is acting as a controller or a processor in relation to any piece of personal data, consider whether it decides what information is to be collected and stored, how it is to be used and when it should be deleted or altered. If it does, then it is a controller of that personal data. If your organisation is processing personal data on behalf of another organisation, then that other organisation is a controller and your organisation is a processor. Bear in mind that it is possible for an organisation to be a controller and a processor of the same personal data (where it is being processed or used by that organisation in different circumstances). It is also possible for there to be more than one controller of the same personal data.

In order to ensure compliance with Data Protection Law, you should ensure that all staff within your organisation are sufficiently aware of the data protection requirements for the performance of their responsibilities in a way that enables the organisation to be compliant. This can be achieved by ensuring that your organisation has sufficient internal policies and procedures in place that staff receive appropriate training in relation to these policies and procedures and that regular reviews and audits are carried out.

As an example, the following policies and notices could be put in place:

- Data Protection Policy setting out the steps taken to ensure compliance with the obligations under Data Protection Law;
- Data Subject Access Request Policy setting out the steps to be taken to deal with access requests received from individuals;
- Record Retention Policy setting out retention periods for different types of records and information and when they should be deleted; and
- Data Security Breach Procedure setting out what to do if a security incident occurs in relation to personal data held by your organisation (e.g. in the case of an unauthorised disclosure, or loss or theft of a device).

Separately, your organisation should have appropriate notices in place to ensure that individuals are made aware of what personal data it collects and how it is used. These may include data protection/privacy notices for employees and contractors, for clients or service users and for visitors to your organisation's website.

Controller Obligations

If your organisation is a controller of personal data, it should be aware of its obligations in the following areas:

Principles of data protection

Controllers should comply with seven key principles, which underpin data protection law:

a. Lawful, fairness and transparency

The processing of data must be done in a lawful, fair and transparent manner. Data subjects should be given clear and intelligible information about how their data is collected, used, consulted and otherwise processed.

b. Purpose limitation

Personal data should only be collected for specific, explicit and legitimate purposes and cannot be further processed in a manner that is incompatible with those purposes.

c. Data minimisation

Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed.

d. Accuracy

Data must be accurate and kept up to date.

e. Storage limitation

Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary. To this end, controllers should establish time limits for erasure or periodic review of personal data.

f. Integrity and confidentiality

There must be appropriate technical and organisational measures in place to protect against unauthorised or unlawful disclosure, destruction or damage of personal data. g)

g. Accountability

The controller is responsible for, and must be able to demonstrate, compliance with Data Protection Law.

Case Study:

A December 2020 decision of the DPC considered the data minimisation principle. While this decision, concerning Groupon International Limited, had a cross-border element, the decision ultimately concerned Groupon's practice at the time of requiring data subjects to verify their identity with an electronic copy of a national identity card. This requirement did not apply when data subjects created a Groupon account but applied when data subjects made certain requests, including requests for erasure of personal data. The DPC found that Groupon infringed the principle of data minimisation by requiring the complainant to verify their identity by submitting a copy of a national ID document in circumstances where a less data-driven solution to the question of identity verification was available. For example, Groupon could have instead required email verification. The DPC's decision is available here: https://www.dataprotection.ie/en/dpc-guidance/law/decisions/groupon-december-2020.

Lawful processing

In order to process personal data, you must have a lawful basis to do so. The lawful grounds for processing personal data are:

a. The consent of the individual;

b. The processing is necessary for the performance of a contract with the individual;

c. The processing is necessary for compliance with a legal obligation;

d. The processing is necessary to protect the vital interests of the data subject or another person;

e. The processing is necessary for the performance of a task carried out in the public interest; or

f. The processing is necessary for the purposes of legitimate interests pursued by your organisation or a third party (except where those interests are overridden by the interests or rights and freedoms of the data subject).

If your organisation intends to rely on consent as a legal basis, it must ensure that the consent is freely given, specific, informed, unambiguous and in plain language. Consent will not be regarded as freely given if the data subject is unable to refuse or withdraw consent without detriment, which is often the case, for example, in an employer/employee relationship. If processing has multiple purposes, consent should be obtained for each of these purposes. Your organisation should keep a record which can demonstrate that consent was received.

For consent to be informed, the individual should be aware of the identity of the controller and the purpose of processing. Your organisation should seek unambiguous consent, for example by requiring data subjects to tick a box or to provide some other form of statement or conduct which clearly indicates consent. Your organisation cannot regard silence or inactivity as consent and the use of pre-ticked boxes should be avoided.

Where a person, by reason of age or incapacity, cannot give valid consent, then consent may be provided on their behalf by their parent or guardian.

Special categories of personal data

Generally, the processing of any of the special categories of personal data (mentioned at the outset of this guide) is prohibited except where:

a. The data subject has granted their explicit consent to the processing;

b. The processing is necessary in order to carry out your obligations in relation to employment, social security or social protection law;

c. The processing is necessary to protect the interest of the data subject, or another person;

d. The processing relates to data that has been made public by the data subject; or

e. Other limited exceptions apply, such as to establish, exercise or defend legal claims.

If you are a not-for-profit body, you may process special category personal data in the course of your legitimate activities, provided that there are appropriate safeguards in place and the processing relates solely to your members, past members or individuals that are in regular contact with the organisation in connection with its activities.

Transparency

Where your organisation processes personal data, it must provide data subjects with information about that processing. At a minimum, your organisation should communicate the following information to data subjects:

- Who you are and what you do;
- Why you are processing the data;
- Information on the purpose and lawful basis for processing;
- If you are relying on legitimate interests as your legal basis for processing, you must explain what the legitimate interest is;
- If you rely on consent as your legal basis for processing, you must explain that consent can be withdrawn;
- If there is a legal obligation to provide the data, that must be explained;
- Whether you plan on further processing the personal data for a purpose other than the original one;
- How long the data will be stored;
- Whether or not the data will be transferred on to other organisations or individuals;
- If you are transferring the data outside of the European Economic Area (the "EEA"), you must explain why and provide information on the safeguards that will be put in place in relation to that data;
- The existence of the individual's rights under data protection, including the rights to access, correction, erasure, restriction, objection and portability;
- The right to lodge a complaint with a supervisory authority;
- The contact details of your organisation's Data Protection Officer ("DPO"), if it has one; and
- If you are processing by means of automated decision-making, you must provide information about the logic underpinning the automated process, and any consequences arising out of a decision that has been arrived at through automated means.

As mentioned above, your organisation may wish to convey this information by way of a

suitably worded data protection/privacy notice.

Accountability obligations

Your organisation should document its compliance with Data Protection Law. To this end, your organisation should maintain records in relation to:

- The types of personal data it processes;
- The means and purposes of processing personal data;
- Processes aimed at tackling data protection issues at an early stage when building information systems or responding to data breaches; and
- The presence of a Data Protection Officer (if required).

There is a requirement under Data Protection Law to keep *a record of all the processing activities* carried out by your organisation (a "**ROPA**"). This obligation exists whether your organisation is a controller or a processor. A ROPA should include:

- Your organisation's name and contact details, whether it is a controller or a processor (and where applicable, the joint controller, their representative and the DPO);
- The purposes of the processing;
- A description of the categories of individuals and of personal data;
- The categories of recipients of personal data;
- Details of transfers outside the EEA, including a record of the transfer safeguards in place;
- Retention policies; and
- A description of the technical and organisational security measures in place

Organisations with fewer than 250 employees are exempt from keeping a record, but only if the processing is not likely to pose a risk to the rights and freedoms of the data subject, if no special categories of data are processed and if the processing is carried out only occasionally.

Data protection by design and default

Data Protection Law requires organisations to put in place appropriate technical and organisational measures to implement data protection principles effectively and safeguard individual rights. This is 'data protection by design and by default'. Data protection by design means embedding data privacy features and technologies directly into the design of any product, service or process at an early stage. Data protection by default means that data protection friendly settings should apply by default (for example only the data necessary should be processed, short storage period, limited accessibility, etc.).

Risk based approach

When your organisation processes data, the individuals whose data you are processing may be exposed to risks. In particular, the unauthorised disclosure or loss of that data could subject individuals to reputational damage, fraud, discrimination and financial loss. It is important that your organisation takes steps to mitigate these risks. One of the ways to achieve this is through determining the risk profile of all personal data your organisation processes, according to factors

such as the complexity and scale of the processing, the sensitivity of the data and the protection required for the data. Your organisation should maintain a risk register, which will help in identifying and mitigating the risks associated with processing and which may be used to demonstrate compliance in the event of a regulatory investigation or audit.

Before starting a new processing operation, your organisation must also consider whether a Data Protection Impact Assessment ("DPIA") is necessary. A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. A DPIA does not have to eradicate all risks associated with the project, but it should assist your organisation in minimising these risks and in determining whether or not the level of risk is acceptable. A DPIA is mandatory where data processing "is likely to result in a high risk to the rights and freedoms of natural persons". The General Data Protection Regulation provides some non-exhaustive examples of when data processing is likely to result in high risk, such as:

Systemic evaluations of personal aspects of an individual carried out through automated processing and resulting in decisions which can produce legal effects, or effects of a similar kind:

- Large scale processing operations of special categories of data or data concerning criminal convictions;
- Large scale, systemic monitoring of a publicly accessible area;
- Processing biometric data to identify or allow the identification of someone; and
- Systemically monitoring or tracking an individual's location or behaviour.
- DPIAs do not need to take a particular form, though they must contain, at a minimum, the following elements:
- A description of the envisaged processing operations and the purposes of the processing;
- An assessment of the necessity and proportionality of the processing;
- An assessment of the risks to the rights and freedoms of data subjects; and
- The measures envisaged to address the risks and demonstrate compliance with Data Protection Law.

In most cases, there are some data protection risks that cannot be eliminated or reduced. Your organisation can accept these risks if they are proportionate to the benefits that will be achieved by proceeding with the processing activity. You should record any decisions to accept data protection risks. If the DPIA results in the conclusion that the processing would result in a high risk to data subjects, which cannot be managed through protective measures, you should contact the Data Protection Commission before proceeding with the processing.

You should keep a record of the DPIA and aim to review it regularly in order to assess whether the protective measures implemented are succeeding in mitigating data protection risks. If the purposes, or scope, of the data processing changes over its lifetime, it may be necessary to assess whether a further DPIA is required.

Case Study:

The Personal Injuries Assessment Board ('PIAB') reported a personal data breach to the DPC which occurred when a consultancy provider sent an unencrypted USB storage device containing personal data to PIAB. The DPC's decision found that the consultancy provider had failed to meet the requirements of the GDPR by failing to implement a level of security appropriate to the risk presented by its processing of personal data. The DPC's decision is available here:

https://www.dataprotection.ie/en/dpc-guidance/law/decisions/consultancyprovider-january-2022

Security

Your organisation must implement technical and organisational measures to ensure a level of security appropriate to the risks identified. This obligation applies to both controllers and processors under Data Protection Law. Suitable measures may include:

- The encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Data breach reporting

Your organisation must report any personal data breaches to the DPC, except where the breach is unlikely to result in a risk to the affected individuals. You must do so without delay and in any event within 72 hours of becoming aware of the breach. If you fail to notify the DPC within this timeframe, you must give a reason for the delay. If your organisation processes data on behalf of a controller, you must notify the controller of the data breach as soon as possible, regardless of the risk involved.

Where a breach is likely to result in a high risk to the affected individuals, you must also inform those individuals without undue delay. You do not need to notify the data subject if the data was protected by certain security measures that make the data unintelligible, such as encryption. Similarly, you do not need to notify data subjects if you have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise. If the notification would require disproportionate effort, you can notify the affected individuals by way of a public communication or similar measure, provided the data subjects are informed in an equally effective manner.

Responding to data subject requests

As mentioned above, individuals have various rights in relation to their personal data. These include the right of access (which is the most commonly exercised right) and other rights such as the right to rectification and the right to be forgotten.

If you receive an access request from a data subject, you must, subject to any applicable exceptions:

- Tell the individual whether you are processing their personal data;
- Provide a copy of the personal data, without undue delay and in any event within one month; and
- Inform the data subject about the processing (such as the purposes of the processing, categories of personal data concerned, recipients of their data, etc.).

You must provide this information to the data subject free of charge and in an accessible format. If your organisation holds a large quantity of data in relation to an individual, you may request that the individual clarifies the request by specifying the information or processing activities to which he or she wants access. You should only do so where it is reasonably necessary to clarify the request and it should not be used as a means of delaying your response to the original request. If the individual refuses to provide clarification, you must still attempt to respond to the original request.

If the data subject requests a copy of all information pertaining to him or her that is held by your organisation, you must comply with this request in full, irrespective of the level of time and effort involved. You can, however, extend the timeframe for responding to the access request by a further two months where the request is complex or where it relates to a large volume of materials. In this case, you should notify the data subject within one month of the request, giving a reason for the delay.

Similar rules and timeframes apply to other data subject rights.

There are limited exceptions to data subject rights, which are provided for in the GDPR and the Data Protection Act 2018. For example, under the Data Protection Act 2018 data subjects' rights do not apply to any personal data that was processed for the purpose of seeking, receiving or giving legal advice or in

respect of which a claim of privilege could be made.

Data Protection Officers

Certain organisations and types of processing require a data protection officer ("**DPO**"). This individual will be responsible for ensuring your organisation's compliance with its data protection obligations. You must appoint a DPO where:

- Your organisation is a public authority or body;
- Your organisation's core activities consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or
- Your organisation's core activities consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

A DPO has specific functions under Data Protection Law and an organisation has specific obligations in relation to a DPO. Where the appointment of a DPO is mandatory, you must publish details of your DPO and provide these details to the DPC.

Many organisations who are not obliged to appoint a DPO choose to appoint a person to perform a role that is similar to that performed by a DPO, even where this is not a legal requirement. To avoid confusion, typically a person performing such a role will be given a title other than DPO, such as data protection manager, privacy officer, etc.

Processors

If your organisation wishes to engage a third party processor, it must engage in an appropriate level of due diligence regarding the processor's measures for ensuring compliance with Data Protection Law and enter into a legally binding contract with that processor, which governs the processing of the data (a "**Data Processing Contract**"). The Data Processing contract should contain, at a minimum, the following information:

- The subject matter, duration, nature and purpose of the data processing;
- The type of personal data being processed;
- The categories of data subjects whose personal data is being processed; and
- The obligations and rights of the Controller.

Organisations may also wish to impose additional obligations on a processor to ensure it enables the controller to comply with its obligations e.g. to inform the controller in the event of a security breach, or an access request etc.

If your organisation is a processor, it should bear in mind that it may only act in accordance with the instructions of the controller.

Data transfers

If your organisation transfers personal data to a country outside the EEA, you must ensure that the data will be subject to equivalent protection in that country. If the European Commission has issued a decision confirming that the recipient country provides an adequate level of data protection (an "**adequacy decision**"), there is no need to take special measures to provide for a transfer to that country. However, if there is no adequacy decision in place, appropriate safeguards must be adopted, which may include, among other things, putting 'standard contractual clauses' in place between your organisation and the recipient of the data. You can find more information on these mechanisms on the DPC's website, available here.

Direct marketing

To the extent your organisation engages in direct marketing, care must betaken to ensure that appropriate steps have been taken under Data Protection Law and the ePrivacy Regulations in relation to such direct marketing. As outlined above, an individual's personal data must only be kept for one or more specified purpose(s), and this must be kept in mind when targeting donors and/or volunteers for campaigns. If an individual has consented to receiving information on a particular campaign, unless they have consented to it, this individual should not be contacted for fundraising purposes.

The individual's consent must be clear and affirmative. You cannot use an opt-out mechanism, or pre-ticked boxes, in seeking data subjects' consent to electronic direct marketing. The individual is free to withdraw their consent at any stage and the individual must be clearly presented with the right to object. In order to avoid breaching the e-Privacy Regulations, you should ensure that all marketing preferences of your data subjects are known, kept accurate and up to date.

There are certain limited circumstances in which you will not require affirmative consent for electronic digital marketing:

a. The product or service being marketed is your own product or service;

b. The product or service being marketed is of a kind similar to that supplied to the individual in the context of the original transaction;

c. The individual must be given the opportunity to object to the use of their details at the time those details are collected, as well as each time you send an electronic marketing message; and

d. The initial direct marketing communication must be sent within 12 months of the date of the original transaction with that individual.

In these circumstances, when their data is being collected, individuals should be given a way to opt-out from receiving any marketing material. This should be drawn to individuals' attention, displayed clearly and separate from any other information, such as terms and conditions. This can be achieved through an 'opt out' box or 'unsubscribe' at the end of marketing emails, for example.

The EU intends to introduce an e-Privacy Regulation which will give data subjects additional rights in this area. Once this Regulation is adopted and brought into force, it will supersede the current ePrivacy Regulations. The finalisation of this Regulation has taken much longer than was intended. At one time it was intended that it would be adopted shortly after the GDPR became applicable in 2018, however it remains a work in progress in the EU legislative process. At the time of writing this guide, it seems unlikely to become applicable before 2025 at the earliest.

Processor Obligations

As processors act on the instructions of controllers, they generally have less autonomy over the data they process. If your organisation is a processor, it must enter into a Data Processing Contract with the controller before commencing its processing activities. As mentioned above, this contract will address a number of compulsory matters but it may also set out additional obligations, with which you must comply. Outside of the Data Processing Contract, you should also be aware of your obligations in the following areas:

a. *Controller's instructions*

You can only process personal data on instructions from a controller (unless otherwise required by law). If you act outside your instructions or process personal data for your own purposes, you will step outside your

role as a processor and become a controller for that processing.

b. *Sub-processors*

You cannot engage another processor without the controller's authorisation. If authorisation is given, you must put in place a contract with the sub-processor with terms that offer an equivalent level of protection for the personal data as those in the contract between you and the controller.

c. *Security*

You must implement appropriate technical and organisational measures to ensure the security of personal data, including protecting against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.

d. *Notification of personal data breaches*

If you become aware of a personal data breach, you must notify the relevant controller without undue delay and assist the controller in complying with its obligations in handling the data breach.

e. *Notification of potential data protection infringements*

If you receive instructions from the controller which, in your opinion, would infringe Data Protection Law, you must notify the controller immediately.

f. *Accountability obligations*

As mentioned above, you must comply with certain accountability obligations, such as maintaining records and appointing a Data Protection Officer.

g. *International transfers*

You must not transfer personal data outside the EEA without the controller's authorisation and without appropriate safeguards in place.

h. *Co-operation with supervisory authorities*

You are also obliged to cooperate with supervisory authorities (such as the DPC), where requested.

Anonymisation

If your organisation anonymises personal data, it will fall outside the scope of Data Protection Law. In doing so, you must take sufficient steps to ensure that it cannot be linked to any identifiable information including, for example, by reference to a code or by linking it with other information that you hold. Effective anonymisation can be difficult to achieve and often data which an organisation believes to be anonymised has merely been pseudonymised and is still covered by Data Protection Law. Pseudonymisation involves data being recorded or amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.

Consequences of a Breach

Administrative Fines

If your organisation is in breach of its obligations under Data Protection Law, such as those relating to legal bases for processing, maintaining records of processing activities and notification of data breaches, it could face fines of up to €10 million, or 2% of the organisation's worldwide annual revenue from the preceding financial year, whichever amount is higher.

For more serious infringements that breach the fundamental principles of Data Protection Law, your organisation could face a fine of up to €20 million, or 4% of the organisation's worldwide annual revenue from the preceding financial year, whichever amount is higher.

The DPC will consider the following criteria in determining whether a fine will be imposed and in what amount:

- The gravity and nature of the infringement;
- Whether the infringement was intentional or the result of negligence;
- Whether the organisation took any actions to mitigate the damage caused to data subjects;
- Whether the organisation had taken any precautionary measures;
- Any relevant previous infringements, as well as compliance with past administrative corrective actions under the GDPR;
- Whether the organisation cooperated with the supervisory authority to discover and remedy the infringement;
- The type and categories of data affected by the infringement and whether it affects any special categories of personal data;
- Whether the organisation proactively reported the infringement to the supervisory authority;
- Whether the organisation followed approved codes of conduct or was previously certified; and
- Any aggravating or mitigating factors, including any financial benefits gained or losses avoided as a result of the infringement.

Other Enforcement Powers

The DPC can issue a warning to controllers and processors if an operation is likely to infringe the GDPR. Where there has been an infringement, the DPC can issue a reprimand, impose a temporary or definitive limitation or ban on processing or withdraw any data protection certification.

Compensation

In addition to the administrative fines mentioned above, data subjects also have the right to seek compensation from organisations that cause them material or non-material damage as a result of an infringement of Data Protection Law.

Free Legal Advice Centres,
85/86 Dorset Street Upper
Dublin 1
Tel: +353 1 887 3630
FLAC Information Line:
1890 350 250
Email pila@flac.ie
www.pila.ie

Principal Office
Riverside One, Sir John Rogerson's Quay
Dublin 2 D02 X576
+353 1 829 0000

New York
One Rockefeller Plaza, 30th Floor
New York, NY 10020
+1 646 952 6001

London
Tower 42, Level 38C, 25 Old Broad Street
London EC2N 1HQ
+44 20 7621 1000

Brussels
40 Square de Meeûs,
1000 Brussels
+32 2 740 0370