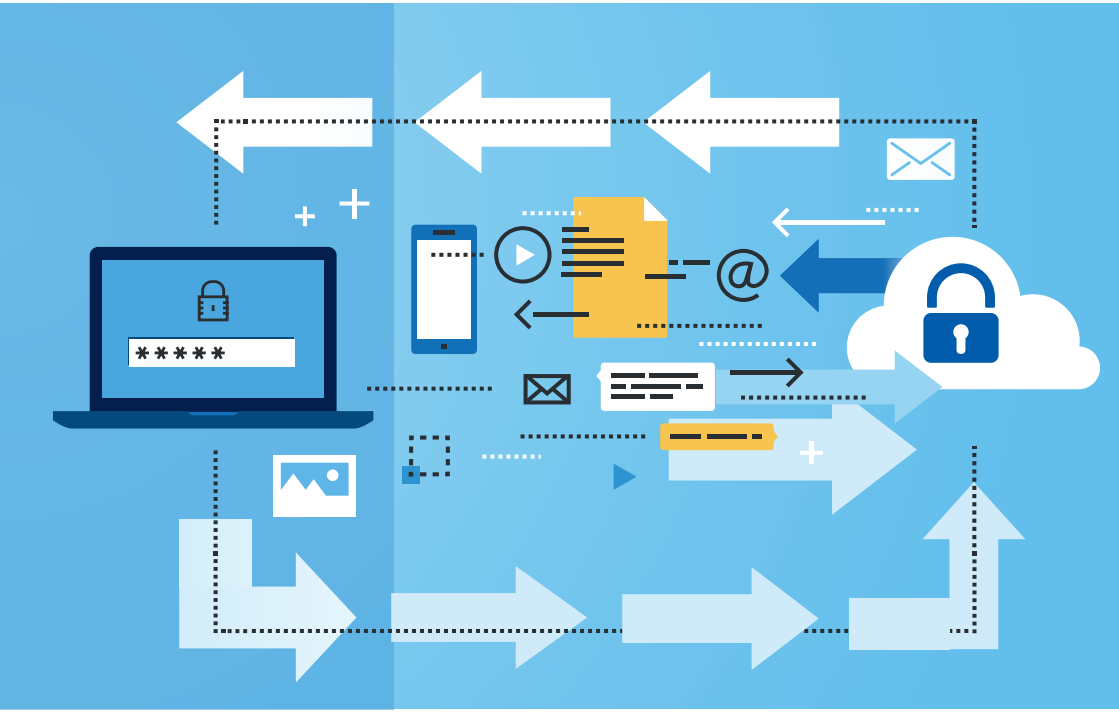
McCann FitzGerald

pila public interest law alliance a project of FLAC

Data Protection

A Handbook for the Not-for-Profit Sector



About McCann FitzGerald

With almost 550 people, including over 350 lawyers and professional staff, McCann FitzGerald is one of Ireland's premier law firms. We are consistently recognised as being the market leader in many practice areas and our pre-eminence is endorsed by clients and market commentators alike.

Our principal office is located in Dublin and we have overseas offices in London, New York and Brussels. We provide a full range of legal services, primarily to commercial, industrial and financial services companies. Our clients include international corporations, major domestic businesses and emerging Irish companies. We also have many clients in the State and semi-State sector.

McCann FitzGerald is proud to support PILA.

About PILA

PILA is a project of FLAC (the Free Legal Advice Centres). PILA is a public interest law network that seeks to engage the legal community and civil society in using the law to advance social change.

McCann FitzGerald

pila public interest law alliance a project of FLAC

Contents

ONE

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 Data Protection Acts 1988 and 2003 (the "**DPA**") and in certain related Regulations. 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. Some further terms are explained in a glossary at the end of this guide.

What is personal data?

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

Who is a data controller?

A data controller is a person or organisation who controls the contents and use of personal data (e.g. an employer in relation to their employee's data, a GP in relation to their patient's data, etc.).

Who is a data processor?

A data processor is a person or organisation that processes personal data on behalf of a data 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 the charity).

Who is a data subject?

Any living individual who is the subject of personal data.

What is sensitive personal data?

Sensitive personal data means personal data as to:

- the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject;
- whether the data subject is a member of a trade union;
- the physical or mental health or condition or sexual life of the data subject;
- the commission or alleged commission of any offence by the data subject; or
- any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

General Data Protection Regulation ("GDPR")

Currently, data protection law throughout the EU is set out in national laws which give effect to an EU Directive, such as the DPA in Ireland. With effect on 25 May 2018, EU data protection law will be overhauled by the GDPR, which will be directly applicable in all EU Member States and which will, broadly speaking, result in a single, uniform set of data protection rules. Many of the provisions of the GDPR are similar to those contained in the existing data protection framework. However it also provides for a number of new rights for individuals, new obligations for data controllers and more serious consequences for failing to comply with data protection law. This guide relates to current data protection law only (as of November 2016) and does not cover the GDPR. Organisations who process personal data should review and update their data protection policies and practices before May 2018 to ensure that they are ready to comply with the GDPR once it comes into effect.

TWO

Data Protection for Individuals

This section of the guide provides an outline of the rights which 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 the DPA only applies to living individuals and does not apply to deceased persons.

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 Commissioner is responsible for monitoring and enforcing compliance with data protection law, including ensuring that your rights as a data subject are respected.

You, the data subject have a range of rights in respect of your personal data which flow from the 8 key principles and which apply where a data controller holds your personal data in digital form, in paper or other manual form as part of a relevant filing system, or both.

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 data controller (e.g. by a letter signed by you confirming that your representative is acting on your behalf).

8 Key Principles of Data Protection

A data controller must:

- Obtain and process information fairly;
- Keep it only for one or more specified, explicit and lawful purposes;
- Use and disclose it only in ways compatible with these purposes;
- Keep it safe and secure;
- Keep it accurate, complete and up-to-date;
- Ensure that it is adequate, relevant and not excessive;
- Retain it for no longer than is necessary for the purpose or purposes for which is was obtained; and
- Give a copy of personal data to an individual, on request.

Rights of a Data Subject

Right to Information

A data controller who obtains your personal data must ensure you are provided with:

- the name of the data controller who is collecting the information or for whom the information is being collected;
- the reason(s) they are collecting your personal data; and
- any other information that you may need to be sure that your personal data is being handled fairly, e.g. details of other organisations or people to whom they give your personal data.

If an organisation/person obtains your personal data from someone else and not directly from you, they must ensure that you are aware of what personal data they hold and how they obtained it.

Right to Access

Under section 4 of the DPA you have a right to ask for a copy of any personal data that an organisation/person holds about you, and you can do this by:

- sending a written request to a data controller;
- including a copy of your ID (e.g. passport or driver's licence); and
- including the maximum statutory fee of €6.35 (where this is required by that organisation/person).

If you make a request that complies with these requirements, a data controller must respond to your request within 40 days. The DPA provides for some limited exemptions to the right of access. For example, a data controller may withhold personal data relating to you which is covered by legal privilege. Subject to these limited exemptions, a data controller should provide you with all personal data relating to you which is within the scope of your request.

Under section 3 of the DPA you can also ask a data controller or data processor to confirm whether they hold any personal data relating to you, and if they do, to give you a description of that data and the purposes for which it is kept. A data controller must respond within 21 days of receipt of such a request made in writing. There is no cost associated with this request, however it is rarely used since most individuals prefer to make a request under section 4 in order to obtain a copy of whatever personal data an organisation holds about them.

Sample Letter

The following is a sample letter which: (a) contains a request for confirmation of any personal data held, and (b) contains a request for a copy of such data:

[INSERT SENDER'S ADDRESS]

[INSERT RECIPIENT'S ADDRESS]

[DATE]

Data Access Request under the Data Protection Acts 1988 and 2003 ("DPA")

Dear Sir or Madam

I am writing to exercise my right, under section 3 of the DPA, to establish the existence of personal data relating to me held by or on behalf of [INSERT THE NAME OF THE DATA CONTROLLER ORGANISATION]. Please confirm whether [•] keeps any personal data relating to me and, if any such personal data is kept, please provide a description of the data and the purposes for which it is kept.

In addition, in exercise of my right to make a data access request under section 4 of the DPA, please send me a copy of all personal data relating to me processed by or on behalf of [•] (whether in electronic or manual form) to date.

I enclose a [cheque/postal order/bank draft] for €6.35 in respect of the maximum prescribed fee, together with a copy of my [driving licence/passport] to confirm my identity.

I look forward to hearing from you in relation to the above as soon as possible and, in any event, within the relevant statutory time limits.

Yours faithfully

[signature]

[insert name]

Right of Rectification or Erasure

You are entitled to request that a data controller, who holds your personal data, rectifies an error in your personal data or erases any such personal data, where it is incorrect or where it has been collected or is being used in a way that does not comply with the DPA.

You should make a request for rectification or erasure in writing, explaining your concerns, and the personal data which you would like to be rectified or erased. The data controller must comply with this request within 40 days of receipt of the request, or respond to your request with an explanation why they will not do as you asked.

Right to Object to Processing Causing Damage or Distress

A data controller may intend to use your personal data for official purposes in the public interest or for their own interests. If any processing for such purposes could cause you substantial damage or distress, you can send a request in writing to the data controller asking them not to use your personal data for such purposes. The data controller must respond to you within 20 days, confirming that they have complied with your request, or explaining why they will not do so.

This right will not apply in certain circumstances, which include if:

- you have already given your explicit consent to the data controller to use your personal data for these purposes;
- the data controller needs to use your personal data for these purposes for the performance of a contract with you; or
- the data controller needs to use your personal data for these purposes for the performance of a legal obligation on the data controller.

Right to Opt-Out of Direct Marketing:

Where your personal data is collected or used for the purposes of direct marketing, you have the right, under the DPA to make a request (in writing) that a data controller:

- does not process the data for the purposes of direct marketing; or
- stops processing the data for the purposes of direct marketing.

A data controller must deal with such a request regarding use of your personal data for direct marketing purposes within 40 days.

You also have a right to opt-out of all direct marketing that is sent to you, including by way of telephone calls, SMS messages or email. Under the ePrivacy Regulations (S.I. 336 of 2011), anyone who engages in direct marketing by electronic means should enable you to opt-out of receiving direct marketing messages both when they collect your contact details and in each marketing message they send to you. If you receive a marketing phone call, you can ask the caller not to call you again and to remove your contact details from the relevant contact list.

In some instances personal data used to market to you is already in the public domain (e.g. in a telephone directory), however you can control how that information is used by marketers and can request that your telephone service provider makes a note of your preference not to receive marketing calls on the National Directory Database 'opt-out' register.

Right to Freedom from Automated Decision Making

Important decisions about you based on your personal data (e.g. your work performance or creditworthiness) should, subject to certain exemptions, have a human input and may not be based solely on automated decision making generated by a computer, unless you have consented to this.

Making a Complaint

If a data 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 maximum time period provided in the DPA, (as set out above, e.g. 20 days for an objection to processing causing damage, 21 days for a request for confirmation of the data held by an organisation or 40 days for an access request, a request for erasure or rectification or a request to opt out of marketing) then you can make a complaint in writing to the Data Protection Commissioner. Except in limited circumstances, the Office of the Data Protection Commissioner will look into the matter for you, free of charge. If your complaint is upheld, the Data Protection Commissioner has the power under the DPA to ensure that the matter is rectified.

If you would like to make a complaint to the Office of the Data Protection Commissioner, you should provide them with as much information as possible to assist an investigation, including, by way of example:

- the identity of the organisation or person about whom you are making the complaint;
- the steps you have taken to exercise your rights and the responses to such steps; and
- copies of all relevant correspondence and any other materials you think would be helpful in demonstrating the organisation or person's failure to comply with the DPA.

Your complaint should be sent to the following postal address:

Office of the Data Protection Commissioner
Canal House
Station Road
Portarlington
Co. Laois R32 AP23

Alternatively, your complaint can be sent by email to: info@dataprotection.ie.

If the Data Protection Commissioner does not uphold your complaint, you will be notified of this in writing. If you disagree with the Data Protection Commissioner's finding, you have a right of appeal to the Circuit Court. This appeal should be made within 21 days from the date of receipt of the letter from the Data Protection Commissioner. The decision of the Circuit Court is final, however an appeal may be brought to the High Court on a point of law against a decision of the Circuit Court.

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. The Office of the Information Commissioner 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 the DPA.

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 4 week 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 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. 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.

THREE

Data Protection for Organisations

An Organisation that collects, stores or processes any personal data relating to living people (e.g. customers, employees, donors, volunteers, clients etc.) in digital form (e.g. on a computer) or in a structured filing system, is a data controller, a data processor, or both and has obligations in relation to that personal data under the DPA.

To determine whether your Organisation is acting as a data controller or a data 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 data controller of that personal data. If your Organisation is processing personal data on behalf of another Organisation, then that other Organisation is a data controller and your Organisation is a data processor. Bear in mind that it is possible to be a data controller and a data processor at the same time. It is also possible for there to be more than one data controller of the same personal data.

It is very important to be aware of the status of your Organisation, as the legal obligations that apply to a data controller are more demanding than those which apply to a data processor. A data controller has a number of key responsibilities in relation to the personal data it holds and uses, which include the 8 rules of data protection and certain other obligations which are summarised below. A data processor has more limited statutory obligations, which consist primarily of the obligations to process the personal data in accordance with the instructions of the data controller and to take appropriate security measures in relation to the personal data.

In order to ensure compliance with the DPA, 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 the DPA;
- 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;

- 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 inappropriate 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 notices for employees and contractors, for clients or service users and for visitors to your Organisation's website.

The 8 Rules of Data Protection

❶ Obtain and process information fairly

An individual (the "data subject") must, at the time their personal data is being collected be aware of the name of the data controller (e.g. your Organisation), the purpose(s) for collecting the personal data, the persons or categories of persons to whom the personal data may be disclosed and the data subject's rights in respect of their personal data. Where the personal data is not obtained from the data subject, either at the time their personal data is first processed or at the time of disclosure to a third party, all the above information must be provided to the data subject by the new data controller and they must also be informed of the identity of the original data controller from whom the information was obtained and the categories of personal data concerned. This notification obligation is generally complied with by ensuring that a 'data protection notice' or 'data protection statement' is included in forms, on a website, etc. where personal information is collected. The Data Protection Commissioner's website (www.dataprotection.ie) provides useful guidance materials on drafting notices and statements.

In order for personal data to be processed fairly, it must have been obtained fairly and the processing must be covered by a 'legitimising condition' for processing the personal data. One of the main 'legitimising conditions' is where the data subject has consented to the processing, however consent is not always required as there might be an alternative 'legitimising condition' that can be relied upon. The alternative options include where the processing is necessary for compliance with a legal obligation, or to prevent injury or other damage to the health of the data subject, or where it is in the legitimate interests of the relevant Organisation, provided that the pursuit of such legitimate interests does not have a disproportionate negative impact on the relevant individual.

The rules regarding processing sensitive personal data are more restrictive. The

explicit consent of the data subject will generally be required, unless one of a more limited range of alternative legitimising conditions is available, such as:

- the processing is necessary for the purposes of carrying out obligations and rights in the field of employment law; or
- the processing is necessary to protect the vital interests of the data subject; or
- the processing is necessary for the purpose of legal advice or legal proceedings.

❷ Keep it only for one or more specified, explicit and lawful purposes

Your Organisation must inform the data subject of the reason why it is collecting and retaining their personal data and must make sure that the purpose(s) for which the personal data is being collected is a lawful one.

❸ Use and disclose it only in ways compatible with these purposes

Your Organisation must ensure that it only uses and discloses personal data in a way that is consistent with the purpose(s) for which the personal data is kept. To determine this, consider whether a data subject would be surprised at how their personal data is being used or disclosed.

A data controller must ensure that any data processor processing on its behalf is also following the requirements to only use personal data for the specified or lawful purposes. To ensure this, there should be a contract in place between the data controller and the data processor which sets out the conditions under which the personal data is to be processed.

❹ Keep it safe and secure

Appropriate security measures must be in place to protect against unauthorised access to, alteration, disclosure or destruction of the personal data which is kept. To achieve this, your Organisation should restrict access to personal data on a 'need to know' basis in accordance with a defined policy; ensure that computer systems and all databases are password protected and that there are appropriate back up procedures in operation for computerised data.

In determining the level of security to apply to the personal data, consider the confidentiality and sensitivity of the personal data in question, and the harm that could result from unauthorised disclosure etc. This is particularly important where your Organisation processes and keeps sensitive personal data.

❺ Keep it accurate, complete and up-to-date

This rule can be complied with by ensuring that databases and files are regularly monitored and reviewed, that your computer procedures are adequate and that there is cross-checking applied to the storage of personal data on your systems to ensure that all personal data held is accurate. Organisations should note that data controllers can be liable for damages to an individual for handling, making decisions or taking action on the basis of inaccurate data.

(This requirement does not apply to back-up data which is kept for the limited purpose of replacing other data in the event of data being lost or destroyed).

❻ Ensure that it is adequate, relevant and not excessive

Compliance with this rule should be simple if your Organisation only holds the minimum amount of personal data required for the purpose(s) of your Organisation or business. Periodic reviews should be undertaken in relation to the relevance of the personal data sought from data subjects (e.g. on forms and websites) and also the personal data that the Organisation already holds.

For example, in the case of donor personal data, collection of a donor's date of birth would not be justifiable unless it is necessary in the particular circumstances, e.g. if signing up for a fundraising trip and to prove the data subject is not a minor.

❼ Retain it for no longer than is necessary for the purpose or purposes

For as long as your Organisation holds personal data, the obligations of the DPA will apply. Your Organisation should be clear on how long personal data will be kept and the purpose(s) for keeping the personal data. Once the purpose(s) has ceased, then the relevant personal data should be destroyed, unless your Organisation is under a legal obligation to retain it or has an alternative legal basis for keeping it. A record retention policy should be put in place identifying the appropriate time period for retaining various types of personal data. A member of staff should be assigned with the responsibility for ensuring that files containing personal data are purged once the personal data is no longer required.

❽ Give a copy of his/her personal data to an individual, on request

Where your Organisation receives a data access request, you must respond within 40 days. You may request a fee of up to €6.35, and you must also be satisfied of the requester's identity (e.g. they have provided a copy passport/ driver's licence). Where the request is refused, either entirely or in part, you must include a reason for the refusal and inform the data subject of their right to complain to the Data Protection Commissioner.

Upon receipt of an access request your Organisation is obliged to provide the requester with a copy of all relevant personal data it holds, subject to the statutory exemptions set out in the DPA. The exemptions include where the data is subject to legal professional privilege, where it is kept for the purpose of preventing, detecting or investigating criminal offences, or where it is a confidential expression of opinion about the data subject made by another individual. It is worth noting that the exemptions are to be applied narrowly. If requested, your Organisation must also provide information on the categories of personal data kept and the purpose(s) for processing it, the identity of the persons or other organisation(s) to whom the personal data is disclosed, the source(s) of the personal data (unless contrary to public policy), and the logic involved in any automated decisions. All relevant manual and computer files must be checked in respect of responding to an access request.

In responding to an access request, be mindful that there are Regulations[1] in place which protect the data subject from hearing anything about them which might cause serious harm to their physical, mental or emotional well-being. The Regulations apply to health data and social work data. In relation to health data, this should not be released unless the data controller obtains sign-off from an appropriate healthcare professional. Social work data should not be released if it would be likely to cause serious harm to the physical or mental health or emotional condition of the data subject and any social work data compiled by a social worker other than as an agent of the data controller should not be released without consulting that social worker.

Also, except in limited circumstances you should not release personal data relating to any other individual, unless they have consented to its release. This is particularly important to bear in mind if, for example, you receive a request from one family member and their personal data is mixed with personal data relating to another family member (e.g. husband and wife, parent and child, etc.)

It is a good idea to have a policy in place to deal with access requests so that in the event that your Organisation receives a request, it is handled by the correct individual and the request is dealt with in the most efficient manner and responded to within the statutory time frame.

1 S.I. 82/1989, S.I. 83/1989

Other Obligations

Engaging a Data Processor

Where your Organisation, acting as a data controller, engages a third party to process personal data on its behalf, it must ensure that it has a contract in place with the data processor setting out the conditions under which the personal data can be processed and the minimum security measures that must be in place, and which provides a right for the data controller to inspect/audit the data processor to ensure compliance with the DPA. Your Organisation may also wish to impose additional obligations on a data processor to ensure it enables you to comply with your obligations e.g. to inform the data controller in the event of a security breach, or an access request etc.

Registration

Certain categories of data controllers and data processors must register with the Data Protection Commissioner, unless their entire processing activities fall within one of the broad exemptions set out under Regulations[2] made under the DPA. It is important to determine whether or not your Organisation needs to register, because it is an offence for an Organisation to process personal data if it is required to register and fails to do so.

Most data controllers are covered by the exemptions from registration, provided that their use of personal data is routine (e.g. using personal data relating to employees for employment purposes, using personal data relating to clients for providing them with goods or services, etc.). However processing health data for medical purposes, among other things, is not covered by the exemptions, so Organisations who do this are among those who are obliged to register.

Data Transfers

Where your Organisation intends to transfer personal data to a country outside the European Economic Area[3] which is not recognised by the European Commission as having adequate data protection laws, certain conditions must be met to ensure that an adequate level of data protection is in place. A limited range of countries outside the EEA have been recognised as having adequate data protection laws, so transfers to most countries (e.g. USA, India, China, Australia, etc.) are subject to these rules. If a transfer is to take place outside the EEA, then either the consent of the data subject must have been obtained, or the data controller must ensure that one of the other permitted methods under the DPA for transferring personal data to countries outside the EEA applies. These include where a data transfer agreement, containing 'standard contractual clauses' approved by the European Commission, is entered into between the Organisation based in the EEA and the relevant Organisation outside the EEA. Alternatively,

2 S.I. 657/2007, S.I. 350/1988, S.I. 351/1988

3 The EEA consists of the Members States of the EU plus Norway, Iceland and Liechtenstein.

transfers to the USA may be permitted under the 'EU-US Privacy Shield'.

It is worth bearing in mind that 'transfers' often arise in the context of IT services. For example, if your Organisation uses data hosting or cloud services which are provided from servers or other infrastructure located outside the EEA, then this will involve transfers of personal data outside the EEA. Also, if your Organisation engages IT service providers located outside the EEA to provide services which involve them having remote access from a location which is outside the EEA (e.g. IT support services provided from India) then this will also involve a 'transfer' of personal data outside the EEA.

This is a complex area of data protection law which is in a state of flux as a result of legal challenges against certain permitted methods for transferring personal data outside the EEA. It is advisable to have a clear policy on data transfers in place to ensure compliance with the restrictions that apply.

Marketing

To the extent your Organisation engages in direct marketing, care must be taken to ensure that appropriate steps have been taken under the DPA and the ePrivacy Regulations in relation to such direct marketing. In particular, individuals should be given the opportunity to opt-out, or in some cases specifically asked to opt-in, to receiving direct marketing messages when their details are collected. Under the ePrivacy Regulations an individual must also be given the opportunity to specify their preferences in respect of any marketing communications they receive and to opt-out of receiving marketing communications.

Different types of marketing communications have different consent requirements. Your Organisation should apply consistent methods of opt-ins or opt-outs as appropriate (e.g. providing an 'unsubscribe' opt-out at the end of every marketing email and SMS message) with regards to 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.

It is an offence to engage in unsolicited electronic marketing which is liable to a fine of up to €5,000 for summary conviction or up to €50,000 (for an individual) or €250,000 (for a body corporate) on indictment. Each electronic marketing communication sent in breach of the applicable rules constitutes a separate offence, so if you send a large number of unlawful marketing communications this could result in potential liability for a very large fine. To comply with the law, ensure that your Organisation captures the marketing preferences of all data subjects, and keeps accurate and up-to-date records in relation to such preferences and give individuals the opportunity to opt-out of marketing.

Security Incidents

In addition to the obligation under the DPA to take appropriate security measures in relation to personal data, there is also a Personal Data Security Breach Code of Practice. This Code of Practice is not mandatory, however

the Data Protection Commissioner expects organisations to comply with it. Under this Code, where there is a security breach in relation to personal data (e.g. as a result of the loss or theft of a device on which personal data is stored, or as a result of inadvertently sharing personal data with inappropriate recipients), the relevant data controller may be required to notify the Data Protection Commissioner or the affected data subjects, or both. Further details are available on the Data Protection Commissioner's website at www.dataprotection.ie.

Consent, children and capacity

Where your Organisation processes personal data based on having obtained the consent of the data subject, it is important to bear in mind that special rules apply regarding obtaining consent from minors (i.e. people under 18) and persons who, by reason of physical or mental incapacity, are unlikely to be able to appreciate the nature and effect of such consent. Where a person, by reason of age or such incapacity, cannot give valid consent, then consent may be provided on their behalf by their parent, or guardian, or grandparent, aunt, uncle, sister or brother, provided that such consent is not prohibited by law.

In relation to minors, the Data Protection Commissioner has indicated in guidance materials that:

- for children under 12 consent should be obtained from a parent or guardian;
- for children aged 12 to 17, consent from the child and the parent should generally be obtained, except where the child seems old enough to understand the nature and effect of giving consent themselves, in which case consent from a parent or guardian may not be required; and
- for people 18 or older, they can give consent on their own behalf, unless they are unlikely to be able to understand the nature and effect of giving consent as a result of any physical or mental incapacity.

Anonymisation

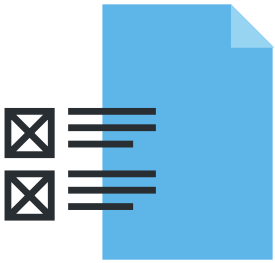
If your Organisation anonymises personal data, in order for this data to fall outside the scope of data protection law, you should ensure that sufficient steps are taken to ensure that it cannot be linked to any identifiable information e.g. by reference to a code or by linking it with other information that you hold. Effective anonymisation can be difficult to achieve and often data which an Organisation believes to be anonymised and outside the scope of the DPA has merely been pseudonymised and is still covered by data protection law.

Exemptions

Section 8 of the DPA sets out limited exemptions to the general obligations on data controllers. Where these apply, an Organisation may process personal data in a way that might otherwise be contrary to one or more of the 8 data protection rules or other obligations summarised above. These exemptions include where the processing is:

- in the opinion of a senior member of the Garda Síochána or Defence Forces, required for the purpose of safeguarding the security of the State;
- required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of the obligations would be likely to prejudice any of these matters;
- required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property;
- required by or under any enactment or by a rule of law or order of a court;
- required for the purposes of obtaining legal advice or for the purposes of, or in the course of, legal proceedings in which the person making the processing is a party or a witness; or
- made at the request or with the consent of the data subject or a person acting on his behalf.

These exemptions can be important if, for example, your Organisation needs or wants to use personal data for a particular purpose but that purpose is not covered by the steps taken by your Organisation to comply with its fair collection and processing obligations. For example, the disclosure of information relating to the suspected commission of a crime to the Gardaí or another appropriate public authority would be permitted under the second exemption mentioned above, despite the relevant individual not being aware of the disclosure of their personal data to the Gardaí for this purpose.



Consequences of a breach

The Data Protection Commissioner is responsible for monitoring and enforcing compliance with the DPA. She has a wide range of enforcement powers to ensure that the principles of data protection are being observed. These powers include the ability to serve legal notices compelling data controllers to provide personal data or to implement one or more provisions of the DPA in a particular manner.

The Data Protection Commissioner may investigate complaints made by the general public or carry out investigations proactively. She can authorise officers to enter premises and to inspect the type of personal data kept by an Organisation, how it is processed and the security measures in place. An Organisation and its staff must co-operate with any such inspection.

In most cases, a breach of the DPA will not, of itself, amount to a criminal offence, whereas a failure to comply with an enforcement notice or information notice issued by the Data Protection Commissioner is an offence. A person found guilty of an offence under the DPA can be fined amounts up to €4,000 for summary conviction and up to €100,000 on conviction on indictment and/or may be ordered to delete all or part of the personal data which is being processed in breach of the DPA. A director, manager, secretary or other office of a corporate body may be personally liable for an offence committed by that corporate body, if the offence was committed with their consent or connivance or was attributable to their neglect.

In addition, an Organisation which is found to have breached the DPA may be 'named and shamed' by the Data Protection Commissioner in her Annual Report or on her website, or both.

Although this guide is not intended to cover the GDPR, it is worth highlighting that potential fines for breaches of data protection law will increase significantly from 25 May 2018 once the GDPR comes into force. Breaches of the GDPR may result in fines of up to the greater of €20,000,000 or 4% of the relevant undertaking's total worldwide annual turnover of the preceding financial year.

Glossary of Terms

Automated data means, broadly speaking, any information on a computer, or information recorded with the intention of putting it on a computer.

Cookies means a small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing a website.

Data means information in a form which can be processed. It includes both automated data and manual data.

Manual data means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.

Processing means performing any operation or set of operations on data, including:

- obtaining, recording or keeping data,
- collecting, organising, storing, altering or adapting the data,
- retrieving, consulting or using the data,
- disclosing the information or data by transmitting, disseminating or otherwise making it available,
- aligning, combining, blocking, erasing or destroying the data.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information is accessible.

McCann FitzGerald

pila public interest law alliance a project of FLAC

McCann FitzGerald

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

Also at London, New York & Brussels

Email inquiries@mccannfitzgerald.com

www.mccannfitzgerald.com

PILA

Free Legal Advice Centres,
13 Lower Dorset Street
Dublin 1
Tel: +353 1 872 8048

FLAC Legal Information & Referral Line: 1890 350 250 / 01-874 5690

Email info@pila.ie

www.pila.ie