The upcoming General Data Protection Regulation (GDPR) signals a new generation of data protection laws which will impact charities and Not-for-Profits (NfPs), effecting how they collect, store and use personal data. While there is reportedly much fear over the potential negative impact GDPR could have and aside from the extra work it might cause, Charities Institute Ireland welcomes this new regulation and believes it offers charities/NfPs an opportunity to truly engage transparently and fairly with donors, sponsors and beneficiaries who can trust charities to keep their personal data safe and secure and use it only for the purpose(s) intended. As part of good governance charity/NfP Trustees should review compliance with GDPR at intervals.

This document is designed to be used as informal guidance and more particularly as a starting point for our members and the wider sector as they become familiar with the obligations that will be imposed on them by the GDPR. We hope that this will assist in identifying some of the key areas of the GDPR of which we think may be of importance to our members. The content of this document was prepared having regard to information that was available at the time of writing and where possible will be updated when further information is issued from the Office of the Data Protection Commission and from the Article 29 Working Party.

PLEASE NOTE: The information provided in these ‘Notes’ represents the views of Charities Institute Ireland. It does not constitute or purport to be legal advice, and does not offer a comprehensive review of the GDPR. You should always consult your legal adviser or a solicitor if you need or think you might need legal advice.
Introduction

GDPR provides for the legal obligations for the protection of personal data. It promotes a risk-based approach to assessing risk when processing personal data. A risk-based approach does not eliminate all risk but rather encourages organisations to evaluate the potential risks and use procedures to control and minimise high-risk processing and the possible impact on individuals of that processing. The GDPR does not indicate how organisations should assess and quantify risk. Charities and NfPs will have to defend their decision to proceed with data processing in light of any risks they have identified and document those decisions. In making such a decision, the issue of ‘proportionality’ i.e., the rights of the individual versus the purpose, interest or benefit of the charity/NfP will have to come into play.

The GDPR applies to personal data if it is processed wholly or partly by automated means or is part of a sophisticated hard copy filing system.

GDPR Terms & meanings - (https://gdpr-info.eu/)

Personal Data/Personally Identifiable Information - is information relating to an identified or identifiable natural person. It is a broad term and includes a wide range of information. The Regulation further states that it includes online identifiers such as IP addresses and cookie identifiers.

Special Categories of Data (previously referred to sensitive personal data) - is personal data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person’s sex life or sexual orientation.

Data Controller - is the legal person (most charities or NfPs will be data controllers) who, alone or jointly with others, determines the purpose and means of the processing of personal data. In other words, the controller (charity/NfP) decides ‘what personal data will be processed for and ‘how’ it will be done.

Data Processor - is the legal person such as an individual or a company who processes personal data on behalf of a controller for example, payroll provider, cloud provider, HR provider if outsourced, direct marketing company etc.

Data Subject - is the individual to whom the personal data relates.

Processing - processing is a very broad concept and includes almost anything you can do with personal data, including collection, storage, use, disclosure and destruction.

Large scale processing - there is little guidance within the GDPR on what large scale processing means. The GDPR suggests that it means processing a considerable amount of personal data which could affect a large number of individuals. Large scale processing sets in motion other elements of the GDPR including Data Protection Officers (DPO) and Data Privacy Impact Assessments (DPIAs).

Risk to individuals - there is a ‘risk’ to the rights and freedoms of individuals if processing could lead to physical, material or non-material damages and includes profiling or processing that could lead to discrimination, identity theft, damage to the reputation etc. It includes any processing of special categories of data or personal data about children or other vulnerable persons or processing that involves large amounts of personal data.

High Risk to individuals - there is little guidance in GDPR on what on what constitutes ‘high risk’ or when processing will be of high risk to individuals.
Processing Principles & Accountability (Article 5)

When processing personal data, a charity which is a data controller must comply with all of the following principles (the first six being in-line with the previous data protection directives)

1. Lawfulness, fairness and transparency – Personal data must be processed lawfully, fairly and in a transparent manner.

2. Purpose Limitation. Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Data minimisation – Personal Data must be adequate, relevant and limited to what is necessary in relation to purposes for which they are processed.

4. Accuracy – Personal data must be accurate and, where necessary, kept up to date. Inaccurate personal data should be corrected or deleted.

5. Retention – Personal data should be kept in an identifiable format for no longer than is necessary.

6. Integrity and confidentiality – Personal data should be kept secure.

7. Accountability – An important change for Data Controllers. Under the GDPR, charities/NfPs must not only comply with the above six general principles but must be able to demonstrate that they comply by documenting and keeping records of all decisions.

NB - Processing Conditions

For the processing of personal data to be lawful under GDPR, charities/NfPs will need to identify the lawful basis for processing personal data (principle 1 above) and document this. The processing of personal data will only be lawful if it satisfies at least one of the processing conditions listed below. Where ‘Special Categories of Data’ is processed, at least one processing condition must also be satisfied.

You must identify the processing condition you are relying on in your privacy notice. If you are relying on the legitimate interest condition, you must include details of that legitimate interest. If you are relying on consent, you must inform individuals of the right to withdraw consent.

Charities/NfPs can employ more than one processing condition for different processing activities and no one lawful basis take precedence over another and will depend on the personal data being processed and the purposes for processing.

Processing Conditions - Processing of personal data (Article 6.1)

- Consent. The consent from the individual must be freely given, clear, and unambiguous.

- Legitimate Interests. The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual. In practice, this may a difficult condition to assert.

- Necessary for performance of a contract. The processing is necessary for the performance of a contract with the individual, or in order to take steps at the request of the individual prior to entering into a contract.
- Legal obligation. The processing is necessary for compliance with a legal obligation to which the controller is subject.

- Vital Interests. That processing is necessary in order to protect the vital interests of the individual or of another natural person. This may also be a difficult condition to assert in practice.

- Public functions. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

**Processing of Special Categories of Personal data (Article 9)**

The Regulation places much stronger controls on the processing of ‘special categories of personal data’. Any processing of ‘special categories data’ must satisfy at least one of the following conditions.

- Explicit Consent - The individual has given their clear and unambiguous explicit consent.

- Legal obligation related to employment - The processing is necessary for the purposes of carrying out a legal obligation and exercising specific rights of the charity/NfP or of the individual in the field of employment, social security law or for a collective agreement.

- Vital interests - The processing is necessary to protect the vital interests of the individual or of another person where the data subject is physically or legally incapable of giving consent.

- Not-for-Profit bodies - The processing is carried out in the course of the legitimate activities, with appropriate safeguards by the Not-for-Profit body and on condition that the processing only relates to members or related persons, or to former members of the body, or to persons who have regular contact with it in connection with its purposes and the personal data is not disclosed outside that body without consent.

- Public Information - the processing relates to personal data which is manifestly made public by the individual.

- Legal Claims - The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

- Substantial public interest - The processing is necessary for reasons of substantial public interest.

- Healthcare - The processing is necessary for the purposes of preventive or occupational medicine, (i.e., healthcare purposes), for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Irish law, or pursuant to contract with a health professional and is subject to suitable safeguards.

- Public Health - The processing is necessary for reasons of public interest purposes and is subject to suitable safeguards.

- Archiving - The processing is necessary for archiving scientific or historical research purposes or statistical purposes and based on EU or Irish law.
The following are some of the rights of individuals under the GDPR:

- Access to the personal data held on them by a data processor or a data controller
- To have inaccuracies corrected
- To have their personal data erased
- To object to direct marketing or other uses or processing of their personal data
- To restrict the processing of their personal data; and
- Data portability

Of the rights of individuals, it is worth noting that the following are qualified rights:

- The right to have their personal data erased - to be upheld unless the processing is necessary:
  
  (a) to exercise the right of freedom of expression and information;
  
  (b) for compliance with a legal obligation which requires processing by a law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
  
  (c) for reasons of public interest in the area of public health;
  
  (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
  
  (e) for the establishment, exercise or defence of legal claims.

- The right to object to processing - to be upheld unless:
  
  (a) the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject; or
  
  (b) for the establishment, exercise or defence of legal claims.

- The right to restrict processing, to be upheld where:
  
  (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
  
  (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
  
  (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

  the data subject has exercised their right to object to processing, and pending the verification whether the legitimate grounds of the controller override those of the data subject.
Section 1

Consent

(There are some conflicts around ‘consent’ within the GDPR Regulation. Charities Institute Ireland made a submission to the ODPC on March 30th that was forwarded to Article 29 Working Party. It is anticipated that the Article 29 Working Party will issue its European-wide guidelines on consent later this year. This element of our notes will be updated when these guidelines are issued.)

Obtaining consent from an individual is only one legal basis for a data controller to justify processing a data subject’s personal data. The GDPR imposes onerous requirements where a data controller relies on consent to process personal data and seeking consent will only be appropriate if the individual has a genuine choice over the matter. For the sake of clarity, the GDPR consent provisions can be boiled down to a few basic points, namely:

1. Consent remains a lawful basis to transfer personal data under the GDPR;
2. A person needs to signal agreement by “a statement or a clear affirmative action.” Silence, pre-ticked boxes or inactivity do not constitute consent.
3. The consent must be freely given, specific, informed and unambiguous. If required to do so, the organisation must be able to demonstrate that the individual has in fact consented;
4. The consent must be as easy to withdraw as it was to give in the first place and organisations must inform data subjects of the right to withdraw before consent is given.
5. The consent language must be intelligible and in an easily accessible form, using clear and plain language.
6. The request for consent must be clearly distinguished from other matters contained in the document or website.

It will be much harder for charities/NfPs to obtain a valid consent with the purpose for data processing attached to that consent and individuals having the right to withdraw their consent at any time. Your charity/NFP must keep records so it can demonstrate that consent has been given by the relevant individual. (Affirmative action, the consent must consist of a clear affirmative action. Inactivity or silence is not enough, nor pre-ticked boxes. Generally, implied consent is no longer sufficient to demonstrate a legal basis for processing, however, consent through a course of conduct remains valid, i.e., a continuous donation via standing order/direct debit etc), until such time as the consent has been withdrawn.

Consent must be explicit if you are processing ‘special categories of personal data’, i.e., the individual ticking a box containing the express word ‘consent’. If your charity/NFP processes sensitive personal data using consent, your organisation needs to address how it will record this type of consent separately from direct marketing. Explicit consent cannot be obtained through a course of conduct.

If your charity/NFP decides to rely on consent for an activity, you should review the way you obtain consent to confirm it meets the requirements of the GDPR, i.e., you are not using pre-ticked boxes and the request for consent is separate from other matters and not buried in a Privacy Policy or
Privacy Statement. A full transparent disclosure of the purpose for collecting and use of the personal data must likewise be clear and provided to the data subject at the point of consent, and again not buried in a Privacy Policy or Privacy Statement. You will also need a process to record consent, document it and manage requests to withdraw consent. Consideration needs to be given to what channels your charity/NfP makes available for a withdrawal of consent? How will you record and act on that withdrawal? If consent is withdrawn, are there any other lawful processing conditions you can rely on.

**Retrospective Consent.**

Where consent has been given under the previous Data Protection Directive, it will continue to be valid under the GDPR if it also meets the new requirements as outlined in GDPR. However, this may be difficult given the new and stringent requirements around consent. Charities/NfPs will have to verify the quality of the consent they have previously obtained for existing and future data processing activities. If these consents fail to meet the standards imposed by the GDPR, organisations will either have to request new consent or seek another legal basis for the processing of personal data as outlined above. *(Please see our Frequently Asked Questions below for further information)*

**Consent and Children**

*(The GDPR specifically states that consent is not necessary when providing preventive or counselling services to a child).*

Ahead of the GDPR, the Irish Government recently set the digital age of consent for a child at 13. Consent from a child (below the age of 13) in relation to online services will only be valid if authorised by a parent. There are other protections for children limiting the situations in which the ‘Legitimate Interests’ condition applies and providing them with a stronger ‘right to be forgotten’

The GDPR contains some other provisions affecting children in particular:

- Your privacy policies must be very clear and simple if your services or products are aimed at a child
- Profiling and automated decision making should not be applied to children
- The right to be forgotten applies very strongly to children.

If your charity/NFp collects data from minors, you should give consideration to arrangements for collecting and storing parental consent.
**Legitimate Interest.**

Another lawful basis for processing personal data under the GDPR is under ‘Legitimate Interests’ of the Controller.

Article 6 1(f)

‘Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual which require protection of Personal Data, in particular where the data subject is a child.

Recital 47

‘The legitimate interests of a controller, including those of a controller to which the Personal Data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject at not overriding, taking into consideration the reasonable expectation of data subjects based on their relationship with the controller.

Legitimate Interests may be considered where:

- another Lawful Basis is not available
- Where there are a number of lawful bases that could be used but ‘Legitimate Interest’ is the most appropriate.

‘Legitimate Interests’ can only be relied upon as a Lawful Basis of processing to the extent that such activity is ‘necessary’. When evaluating whether processing is ‘necessary’ charities/NfPs will need to take into account whether on balance their ‘legitimate interests’ are outweighed by the rights and freedoms of the data subject and the processing would not cause unwarranted harm. This is called a ‘balancing test’ or a Legitimate Interests Assessment (LIA) (Article 7(f) (Charities Institute Ireland will issue guidance later on the ‘Balancing Test and conducting an LIA’). By conducting LIA & Balancing Test, a charity/NfP can ensure that the privacy rights of individuals are given due consideration. In order to ensure compliance with Article 5(2) of the GDPR it is necessary for charities/NfPs to maintain a written record that your charity/NfP has carried out an LIA and the reasons why it came to the conclusions that it met the balancing test elements.

*(Please Note: The fact that a charity/NFP has a legitimate interest in the processing of certain data does not mean that it can necessarily rely on Article 7(f) as a legal ground for the processing. The legitimacy of the Charity/NFP’s interest is just a starting point, one of the elements that need to be analysed under Article 7(f). Whether Article 7(f) can be relied on will depend on the outcome of the balancing test).*

Charities/NfP using ‘Legitimate Interests’ as the Lawful Basis for processing are required to inform individuals that it is processing Personal Data on this basis, what those legitimate interests are and notify individuals of their right to object. (This can be highlighted to an individual at the point of data collection when explaining what ‘legitimate interest’ means and in the section of an E-Privacy Notice that deals with individuals’ rights).
Identifying areas where Legitimate Interests may apply.

Some interests are likely to be legitimate because they are ‘necessary’ for corporate governance or legal and compliance etc., to ensure the charities/NfPs adheres to internal or external governance issues. Other interests are legitimate because they are a routine part of the activities of the charity/NFP and other lawful bases for processing are not practical or not available.

The context of the relationship between the data subject and your charity/NfP is a key element in understanding the legitimacy of the processing activity. ‘Legitimate Interests’ is more likely to apply when there is a direct ‘appropriate relationship’ with individuals because the processing is less likely to be unexpected or unwanted, so the balancing test will be easier. Recital 47 indicates that it is more difficult to use legitimate Interests when there is no pre-existing relationship (although this is not ruled out).

Recitals 47 to 50 in the GDPR gives some examples of when a Data Controller may have a ‘legitimate interest’ which would need to be confirmed by a balancing test/LIA (for the purpose of this guidance, only three are detailed):

- Direct Marketing - Processing for Direct marketing purpose under legitimate Interests is specifically mentioned. Recital 47. (Note: The GDPR says ‘processing of Personal Data for direct marketing purposes may be regarded as carried out for legitimate Interest. A charity may wish to rely upon Legitimate Interests where Consent is not viable or not preferred and the Balance of Interests conditions can be met. The GDPR states ‘maybe regarded as….’ So charities will still need to ensure that they can establish ‘necessity’ and balance their interests with the interests of those receiving the direct marketing communications).

- Reasonable Expectations – The fact that individuals have a reasonable expectation that the Controller will process their personal data will make the case for ‘legitimate interest’ to apply when conducting the balancing test.

- Relevant & Appropriate Relationship. – where there is a relevant and appropriate relationship between the individual and the Controller in situations where the individual is a client or in the service of the organisation. However, this does not mean that there will always be a Legitimate Interest in processing an individual’s data.

The following is a non-exhaustive list of some of the most common contexts in which the issue of legitimate interest in the meaning of Article 7(f) GDPR may arise for charities/NfPs. It is presented here without prejudice to whether the interests of the charity/NFP will ultimately prevail over the interests and rights of the individual when the balancing test is carried out.

- Conventional direct marketing and other forms of marketing or advertisement. Only applies to postal marketing. E-marketing is Consent.

- Unsolicited non-commercial messages, including for charitable fundraising

- For ethical and humanitarian purposes for the assessment and allocation of resources. This is in the interest of both the beneficiary and the charity.

- Individual’s Right to erasure. Charities will need to keep basic data to identify individuals who have requested their information to be deleted and retain it solely for suppression purposes to ensure there is a record of their objection to direct marketing and to prevent further unwanted processing. This activity would be in the mutual interest of the individual who wishes their privacy rights to be upheld and for the charity/NfP to fulfil its right.
- Charities using web analytics to assess the number page views, reviews and followers in order to optimise future marketing campaigns. A charity/NfP relies on consent for marketing communications but may rely on ‘Legitimate Interests’ to justify analytics to inform its marketing strategy and to enable it to enhance and personalise the donor experience.

- Human Resource/Employee relations.

- Processing for research purposes (including marketing research)

**Direct Marketing**

 *(Any direct marketing campaign undertaken by charities/NFP now needs to be GDPR compliant. Any e-Marketing campaigns compliant with the current Privacy and Electronic Communication (EC Directive) Regulations 2003 (PECR)).*

Direct Marketing is a form of advertising which allows organisations to communicate or target directly individuals through a variety of media. Unlike mass advertising which is presented to everyone, direct marketing is presented only to people who are suspected to have an interest or a need for an organisations’ products/services based on the information gathered about them.

Direct Marketing messages involve a specific call to action to a specific person. The results of campaigns are immediately measurable, as organisations can track how many individuals have responded through a message’s ‘call to action’.

The components of direct marketing are:

- Engagement of individual (customers/donors/supporter etc.).
- Specific call to action
- Means of tracking response.

Methods of direct marketing include:

- Mobile phone texting
- Emails
- Websites/Targeted on-line adverts
- Database Marketing
- Fliers
- Newsletters
- Brochures
- Post Cards
- Coupons
- Catalog Distribution
- Telemarketing
- Promotional Letters
All fundraising activity, as well as the promotion “of aims and ideals” and campaigning activity of charities, is covered by the definition of Direct Marketing.

Administrative functions such as donation acknowledgements are not seen as direct marketing. However, it is important to note: the definition of direct marketing also covers any messages which includes some marketing elements, even if that is not their main purpose. In practice, this means that the insertion of an “ask” within a communication which is predominantly administrative, changes the definition of that communication to direct marketing.

All charities/NfPs undertaking direct marketing should consider how they currently understand direct marketing and more importantly what they think isn’t direct marketing and review and define their approach to ensure it meets the legal requirements of the GDPR and establish:

- What Direct Marketing activities your charity wants to use personal information for (Purposes).
- The lawful basis on which you plan to obtain and use personal data, including by what channels of communication you wish to communicate with that person (Lawfulness).
- How your charity will ensure individuals:
  1. are treated fairly;
  2. know about your proposed use (or uses) of their personal information, and
  3. can use their rights to manage their personal information (Fairness and Transparency) i.e. compliance with the 1st principle of Data Protection law

Charities/NfPs should assess what impact direct marketing under the GDPR will have on any existing data management systems, i.e., CRM & other databases to ensure that these systems support the delivery of the agreed approach. Can your charity’s/NfP’s chosen system enable your charity/NfP to capture mail preferences, ‘opt-ins’ and ‘opt-outs’ for all communication channels, capture the date of ‘opt-ins’, ‘opt outs’, or a record of what communications have been received by whom and what date such notifications were received.

Currently, your database needs to record the most recent status of consent for personal data collected. Under the GDPR your charity/NfP will also need to be able to demonstrate ‘unambiguous’ consent. If your charity uses more than one type of consent wording (e.g. for websites, face to face, in-bound call, etc.) we would recommend that you keep an electronic file comprising indicative copies of all past and present consent statements. These will help you meet the GDPR requirement for evidence of consent, in the form of:

- status of consent (e.g. opt-in)
- channel (e.g. for marketing emails)
- the purpose of communications

The next step is to add a field to records on the database identifying which consent statement was used with a time and date stamp.

Be wary of the common practice of operating a retention list, containing personal data of people who have opted-out but that you may intend to contact again in the future with a view to winning them back. This precise scenario led to prosecutions against Topaz (Local Fuels) Limited and Dermaface Limited, the reports of which are available on the website of the Data Protection Commissioner [www.dataprotection.ie](http://www.dataprotection.ie)
Consent and Direct Marketing

The GDPR provisions on consent are a source of concern for many charities. Not only has the definition of consent been significantly amended, the new provisions introduce an element of complexity into what constitutes consent, particularly with regard to the “opt-in” and “opt-out” approaches. For fundraisers, this is a particularly tricky area, especially when it comes to direct marketing. (This is further explored later in these Notes).

Consent can cover all activities which involves personal data processing carried out for the same purpose(s). When processing has different, separate purpose(s), consent is required for each. (“No one fits all” Recital 32) For example, if your charity/NfP receives consent from donors to email updates about the impact of their donation, your charity/NfP cannot send fundraising emails or emails about future campaigns from this consent.

The E-privacy element of the GDPR is still under discussion and is not likely to be finalised until the end of this year or beginning of 2018. The previous e-Privacy Directive which is still in place imposes additional constraints if you market by telephone, email or fax using consent as a default. Charities/NfPs can only send direct marketing to a data subjects if:

- Data subjects have given their (GDPR form of) consent;
- You have an existing relationship with them and falls within the so-called similar products and services exemptions; or
- Data subjects have not opted-out or withdrawn their consent.

In relation to e-marketing, consent should be obtained for every type of communication you want to send donors/supports, and for each channel. For example, if the opt-in tick-box question is worded in the following way; “We would like to email you to keep you updated on the impact of your donation and future fundraising campaigns”, …..and the donor subsequently unsubscribes, you then have to take it that they have unsubscribed from both impact and fundraising emails.

Direct Marketing is an activity that can fall under ‘Legitimate Interest’ for a charity within the (GDPR) and that charities, therefore, do not need to seek consent for postal marketing, once the data has been obtained fairly and lawfully. (Please see sections on ‘Legitimate Interest and Consent v Legitimate Interest further in these notes).

Individual’s Rights - Right to object to Direct Marketing.

The GDPR preserves the right for individuals to object to Direct Marketing. When an individual exercise this right, you must not only stop sending direct marketing material to the individual but also stop any processing of that individual’s personal data for such marketing. For example, if you receive an objection, you should stop profiling that individual to the extent related to direct marketing. The reference to profiling here is new and it is not clear if this is intended to create a wide ranging out from profiling.
Profiling (& Wealth Screening)

(There are some inconsistencies around ‘profiling’ within the GDPR Regulation. Charities Institute Ireland made a submission to the ODPC on March 30th that was forwarded to Article 29 Working Party. The Article 29 Working Party guidelines on profiling are due to be published later this year. Outlined in these notes is the current situation)

What is Profiling?

Profiling is the recording and analysis of a persons’ psychological and behavioural characteristics to enable aspects of their personality or behaviour, interests and habits to be determined, analysed and predicted. It includes behavioural cookies and web analytics, etc.

Profiling under the current Data Protection Legislation

Under the current Data Protection Acts 1988 and 2003 there is no legal definition of ‘profiling’ referring to automated decisions without mentioning profiling ‘the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to data subjects, such as his performance at work, creditworthiness, reliability, conduct, etc… unless such a decision is

- Taken in the course of entering into or performance of a contract; or
- Authorised by law.

Profiling under GDPR.

‘Profiling’ is one of the provisions of the GDPR and is clearly defined under Article 4 (4) as ‘any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements’. This is a very comprehensive definition covering amongst other things - most of the automated decision making commonly used in marketing.

Automated Data - What is automated decision making?

The above definition, Article 4 (4) excludes data processing that is not automated and Article 22 (1) references ‘solely’ automated processing.

‘Profiling’ is then composed of three elements

- It has to be an automated form of processing
- It has to be carried out on personal data
- The purpose of the profiling must be to evaluate personal aspects about a natural person.
The legislation is unclear whether ‘automated processing’ means purely automated, or whether human involvement at any stage no longer qualifies it as processing.

Article 22 of the GDPR sets our three criteria which may trigger the provisions on automated processing of personal data, namely:

- A decision has to be made about an individual
- Which has a legal effect for that individual or significantly affects him or her; and
- This decision must be based solely on automated processing.

Profiling can create new data that needs to be GDPR compliant in its own right. The fact that profiling can use data from a variety of sources (including publicly available sources) create derived or inferred data that raises the following issues;

- How to give effective and timely fair processing; and
- What individuals might reasonable expect

That ‘profiling’ requires some sort of an outcome or action resulting from the data processing is underscored by the individual’s right to be informed of the ‘consequences’ of profiling decisions as discussed in Recitals 60 and 63.

### Profiling for Marketing Purposes

Profiling for marketing purpose will fall outside this restriction as it is unlikely to have legal effects or significantly affect the individual. Charities/NfPs must notify individuals that Direct Marketing Profiling exists, usually via the Privacy Policy. Individuals may have right to object to profiling for direct marketing (subject to clarification in guidance yet to be issued from the Article 29 working party). If an individual opts-out of direct marketing then this must be recorded on your database and in this instance you should not profile them for direct marketing purposes either.

A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data.

### Does Profiling include Wealth Screening

Wealth screening also known as content profiling has proved particularly controversial in the UK. No fine has yet been issued for wealth screening alone, but in each instance where it has formed part of an enforcement case, the charity had failed to be transparent about this activity. This activity in itself is not unlawful, but there will always be risked attached to it, both in reputational terms, and the fact there is not a clear line of compliance. Factors in the balance will be the scale of the activity and the nature of the data used.

### Notice and access.

In the case of profiling decisions subject to Article 22, Article 13 provides that the controller must inform a data subject at the time data is collected, not only the fact that profiling will occur, but as well ‘the logic involved’ and the envisaged consequences of such processing. Under Article 14,
a data subject may also enquire of a controller and receive confirmation of any such processing, including profiling and its consequences, at any time.

Under GDPR a ‘legitimate interests’ argument can/may apply to these activities. This involves a balancing of a charities’ interests against those of the individual, noting in particular, what the individual’s reasonable expectations will be and the active steps taken by the charity to communicate its intentions clearly and transparently.

Charities Institute Ireland advises that opt-in only consents for this activity is the one safe way of ensuring compliance due to what would be considered its intrusive and unexpected nature. If you are profiling/or wealth screening, you will be required to inform donors of this and seek their consent to do so or offer them the option to stop.

Charities Institute Ireland advises our members to review existing privacy notices to ensure they are clear enough for an individual to reasonably foresee how and why you will use their data. An individual’s right at any time to object to and opt out of these activities must be offered, made simple to exercise and respected.

Section 2

Marketing and Fundraising - Consent v Legitimate Interest

The ‘opt-in’ approach

What the new regulation boils down to is a shift from previous guidelines whereby direct marketers could put a reliance on people to opt-out, e.g. by failing to untick a pre-ticked box or by failing to take an action which indicated they want out of receiving direct marketing content. Under the GDPR, marketers must have specific confirmation of a desire to opt-in. Consent therefore requires clear, unambiguous action that shows that the person wants to receive direct marketing information from an organisation, such as your charity. That action must be distinct from the act of donating and be sufficiently positive on the part of the person, as to signify that they consciously ‘opt-in’ to receiving such communication from you.

Such positive action could be in the form of an individual ticking a box or supplying their contact details on a form where it has been made clear that they’re doing so in order to receive direct marketing.

An opt-in will only remain valid where the individual has not opted-out and where the marketing is carried out regularly. Current guidance is that you must be in contact with the individuals at least every 12 months to be able to say that the list is current. If the individuals do not opt-out then you may continue the contact. Note that under proposed changes to the e-Privacy legislation this may change to every 6 months.

With these new provisions, some misconceptions have arisen in some quarters that all direct marketing now needs to be opt-in. However, that is a misunderstanding of the import of the GDPR provisions.

Legitimate Interest

The GDPR leaves room for marketers to use different legal conditions to process data, and one of them, ‘legitimate interest’ is tantamount to an ‘opt out’ mechanism. This legal condition means
that your charity, in certain circumstances, can send direct marketing to a person without their prior consent. However, such a person must have had an opportunity to say ‘no’ or object to future direct marketing, which is often done through an ‘opt out’ tick box.

Article 7 of the GDPR, which focuses on lawful basis for processing data says that data can be processed where “The processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data ...”

It makes clear in Recital 47 that “The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.”

This means that direct marketing may be in the legitimate interests of a charity, making it lawful to process a person’s data without their prior consent. However, this will not always be the case and it’s important to bear the following in mind:

- An individual’s rights and interests override your charity’s legitimate interests in sending them marketing material. Under the GDPR, people have the right to ask organisations not to use their personal information for direct marketing, and you have to respect that.

- You must consider whether, at the time of providing their info, the person would have reasonably expected that their personal information would be used for direct marketing. If not, then it would not be legitimate for your charity to use it for such purposes.

- If the information was collected for a different purpose, or if the individual was not informed that the information would be used for direct marketing you cannot rely on the legitimate interest condition.

From the above, it can be seen although it gives charities some wiggle room, legitimate interest cannot be viewed as carte blanche. It is in fact more of a balancing exercise.

**Positioning your charity to stay in compliance**

To safely rely on legitimate interest you must interrogate your rationale carefully to ensure it can be justified if challenged. You must also be able to show that the person would reasonably have expected that their data would be used to send them direct marketing and you have not overridden rights in doing so.

There are a few steps your charity can take to help it stay within the confines of the GDPR. First, ensure that when you collect people’s details, you let them know in clear terms, how their personal data will be used.

A second step would be to get some outsider insight into how best to approach data usage. For instance, you could carry out a survey of your current supporters to find out what they think of your current communications – content, method, use of data, etc – anything that will help shape your direct marketing approach. Such an exercise will help you understand the reasonable expectations of people who provide their information to you. A caveat here: the views of your current supporters will not necessarily represent that of everyone who comes in contact with your charity, and so such surveys should be seen merely as an indication, rather than a firm statement of what everyone believes. You can manage the different expectations by making effective use of your privacy notice.
Frequently asked Questions.

If a charity has donors on their database that they been emailing regularly but can’t find the evidence of their original consent or if the consent they have doesn’t fit with the GDPRs new, stricter definition; Do these need to be re-asked for consent? Even if the 12-month rule has been followed and there has been an option to unsubscribe on every email and they’ve never opted out?

It would be advisable to try and re-permission contacts to ensure GDPR level of consent, as under the GDPR organisations will need to be prepared to be able to provide proof of consent. However, any re-permissioning should be approached with caution. In the UK the ICO have issued fines against organisations for email communications trying to get opt-in consent, sent to individuals where they don’t have existing consent. Essentially the Regulator in the UK is taking the view that in trying to meet GDPR requirements you can’t break existing rules.

Where organisations have email consent, but not to GDPR level, asking for opt-in consent should be okay. It is obviously more tricky where there is no existing consent. In theory, it will not be compliant to continue using this data once GDPR is enforced.

Charities Institute Ireland would advise with any re-permissioning exercises via email, that small tests are conducted (with relatively low volumes) to gauge reaction/complaints. Obviously, the more engaged the audience (i.e. they’ve opened recent email comms) the less risky.

Using the postal route for re permissioning is much less risky, also we would recommend trying to use any inbound opportunities to trigger re: consent, e.g. pop ups on websites and asking for consent on inbound calls.

How long to store data?

While the donor has the option to ask to have their data removed from our marketing lists, as data Controllers, Charities/NfPs have to ensure that we only store personal data for as long as we need it, which may be for a period of time defined in statute, such as for tax purposes. There is no clear limit on how long data can be kept but you need to be able to explain why you are holding data from a donor who has not communicated with you or donated in the last ten years.

Can donors see the information your Charity/NFP holds on them?

As with the current legislation, donors have the right to access their own data which your charity/ NFP holds on its databases. This option needs to be provided, free of charge, to any person about whom you hold personal data should they make such a Data Subject Access Request. The donor also has the right to be given a description of the information and to be told the purpose(s) for holding their information.

The request should be made in writing or by electronic format. The data controller must respond to the Subject Access Request within 30 days. It is permitted to seek to clarify the scope of the Subject Access Request should the request be overly burdensome or require a disproportionate effort on the part of the data controller to comply with the request. It may also be reasonable to seek additional time to respond, in certain circumstances.
**Information Notes - Article 30 – Data Mapping**

**Do we have to tell an individual that we intend to use their data to send direct marketing to them, and if so, when should we do this?**

Yes, at the point of data collection (and at every subsequent point of communication by making reference to your privacy statement) when consent must be freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

**Can we continue to use cold mailing lists once GDPR comes into force?**

In terms of postal marketing, it is still possible to use direct mail delivered to “the householder” which doesn’t require consent.

In the case of personalised mail, consent is required from the donor. If you are purchasing lists to use in any direct marketing, as the data controller you are responsible for ensuring that you use a reputable list supplier who is operating in line with GDPR. Your data provider needs to be able to demonstrate that they have received informed consent from those on the list they provide to you.

When the list supplier is compiling their lists, they must ask for consent on the specific understanding that the personal data gathered will be shared with third parties. Every category of third party business that the data will be shared with must be listed by the provider at the point of consent being given.

You cannot take the provider’s word for it that this practice has been followed. You, as the data controller, must give clear instructions on this matter and this should also be included within the contract and/or service level agreement held with the list supplier.

**Should we use cold email lists?**

The same measures with list suppliers as above must be taken when purchasing and using cold email lists.

**Should we use cold call lists?**

The same measures with list suppliers as above must be taken when purchasing and using cold call lists.