The Wheel
Good Practice Guides

PREPARING FOR THE GENERAL DATA PROTECTION REGULATION (GDPR)

A Guide for Irish Nonprofits

the wheel
Stronger Charities.
Stronger Communities.

SYTORUS
DATA PROTECTION SPECIALISTS

Preparing for the General Data Protection Regulation (GDPR)

A Guide for Irish Nonprofits

Prepared by

SYTORUS
DATA PROTECTION SPECIALISTS

www.sytorus.com

For members of

the wheel
Stronger Charities.
Stronger Communities.

www.wheel.ie

V1.0 November 2017

Contents

GDPR Guidance Document

This Guidance Document provides an overview of the GDPR for the Irish community, voluntary and charity sector. Mindful that few of the thousands of nonprofit organisations that comprise the sector are likely to recruit an external Data Protection Officer on a full-time basis, this document is written for part-time Data Protection Officers who may not have many resources at their disposal in order to achieve compliance. This guidance document aims to provide a useful summary for this specific audience.

A bit of history

Regulation (EU) 2016/679, or the 'General Data Protection Regulations' (GDPR), needs to be read in a wider legislative context. It draws on principles which were introduced by the Universal Declaration of Human Rights (1948), the European Convention of Human Rights (1950) and the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981).

A piece of European Union legislation, the GDPR reforms and replaces the current legislation in force across the European Economic Area, Directive 95/46/EC. As an EU 'regulation', the GDPR will have direct effect on all Member States from 25 May, 2018.

What is all the fuss about?

Data protection legislation applies to any organisation which gathers, holds or processes the personal data of individuals – this covers information on their name, address and phone number, but can be as detailed as their passport details, date of birth or medical condition.

The obligations apply to organisations of all types, from commercial retailers to social media giants, and government departments to nonprofit organisations.

The GDPR is creating much stir in the regulatory sector as it is a large and complex change of data protection legislation at European level. The Directive 95/46/EC is over 20 years old and technology, data processing and the way we do business have changed dramatically since then. The GDPR will introduce some major changes, including placing liability on organisations to be able to demonstrate their compliance, more detail in the contracts between organisations, and more substantial monetary fines for breaches of the Regulation. By introducing the concept of 'privacy by design', it places the manner in which organisations process personal data at the heart of the day-to-day focus.

Key Definitions

While the GDPR introduces several changes to key concepts in data protection terminology, many of the definitions from the 1995 Directive remain unchanged. **Personal data** continues to be defined as 'any information relating to an identified or identifiable natural person'. A **Data Subject** is 'an identifiable natural person… who can be identified, directly or indirectly, in particular by reference to an identifier'.

Examples of personal data are not just a name or an identification number, but also online identifiers and location data. Crucially, personal data can also be 'one or more factors' combined together, which relate to the 'physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. For example, a photograph or video footage, combined with a caption, employee ID or an identifying scar or tattoo can identify an individual.

The current term 'sensitive personal data' as defined by the Irish Data Protection Acts 1988-2003 will be replaced with so-called **special categories of personal data**, which still include health data, biometric data, genetic data, sexual orientation and religious beliefs. Criminal investigations and an individual's criminal record have been removed from the category, and will be dealt with in a different way by the GDPR henceforth.

Processing continues to be defined as both automated and manual and is broadly interpreted. It can mean 'any operation or set of operations which is performed on personal data or a set of personal data'. You do not need to view the actual data, but transmitting it, backing up a file or destroying data all count as a processing activity, even where the data is encrypted.

A **Data Controller** is a natural or legal person who 'determines the purposes and means of processing of personal data'. A **Data Processor** is a natural or legal person who processes personal data on behalf of the Controller, but is not an employee of the Controller.

Under Irish law, both **Controllers and Processors** are considered to be the legal entities or organisations doing the work, not individuals.

The GDPR introduces the concept of **Joint Controllers**, where two or more controllers jointly determine the purposes and means of processing. The organisations must set out a clear description of their respective responsibilities for compliance with the different GDPR obligations, in particular with regard to the rights of the data subject This might apply where organisations share data between them as peers, in a collaborative manner, rather than the more hierarchical relationship between a Data Controller and a Data Processor.

The Seven Principles

Echoing the current data protection regime, the GDPR relies on seven 'principles' contained in Article 5, which will regulate the processing of personal data. In summary, these are:

1. **Lawful, Fair and Transparent Processing**: processing personal data needs to be based on one or several Lawful Processing Conditions (see below). The Data Subject should have full and transparent knowledge of the identity of the parties to the processing, the purposes of the processing, the recipients of personal data, the existence of Data Subject rights and freedoms, and how to contact the Controller. For example, a Data Controller cannot collect an email address for a newsletter subscription without giving full information on the type of processing which will occur.
2. **Specified and Lawful Purpose**: personal data must be processed only on the basis of one or several specified purposes. For example, data which is collected for the purpose of a newsletter cannot automatically be used to target the Data Subject with regular fundraising campaigns.
3. **Minimisation of Processing**: processing of personal data should be adequate, relevant and restricted to what is necessary in relation to the purposes for which they are processed. Not only will this relieve the organisation of the burden of performing actions on personal data, which are not required or necessary, but it will also reduce the overall risk of data breaches. For example, where a nonprofit organisation wishes to ensure that the Data Subject is not a child, it may not be necessary to collect the date of birth of the Data Subject. A year of birth can be provided or the Data Subject can simply confirm at registration that he or she is over the legitimate age.
4. **Accuracy**: personal data shall be accurate and where necessary kept up to date. Nonprofits should rectify any incorrect data and erase any data, which is known to be erroneous or obsolete. This will result in the Data Controller having greater confidence in the quality of data analysis, reporting and marketing campaigns.
5. **Storage Limitation**: personal data shall be kept in a form which permits the identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed. Anonymisation or deletion is encouraged in order to minimise the length of time that personal data is held by the organisation. Some identifiable data may be kept for statistical, scientific or historical research purposes. It may also be in the public interest to keep such data.
6. **Security and Confidentiality**: appropriate technical and organisational measures will be implemented to ensure a level of security appropriate to the volume and format of the data, its sensitivity, and the risks associated with it. For example, organisations should consider appropriate measures to protect or encrypt data when it is being taken out of the office, or transported between locations for off-site meetings. Technical measures might include password protection on files, encryption of files, CCTV security at their office, etc. Organisational measures might include limiting the amount of data that can be accessed by different teams or departments, so that data is only accessed by those who 'need to know'.
   Nonprofits are encouraged to carry out internal security audits and establish the risks of accidental or unlawful destruction, loss, alteration or disclosure of personal data. This includes transmissions to third parties.
7. **Liability and Accountability**: The Data Controller and the Data Processor will be required to demonstrate their compliance with the GDPR. As with the current legislation, the GDPR requires the Data Controller to continue to exercise reasonable care to ensure that the Data Processor carries out the processing in strict compliance with the GDPR.

Lawful Processing Conditions – Personal Data

Data Controllers will be required to be able to justify their processing of personal data, with reference to Lawful Processing Conditions, provided in the Regulation. Under Article 6 of the GDPR, the processing of personal data (e.g. name, address, mobile number, e-mail address, etc.) will be considered lawful only if at least one of the following conditions applies:

- **Consent**: the Data Subject has clearly and willingly agreed to the processing of their personal data for one or several purposes.
- **Contract**: the processing activity is necessary for the performance of a contract between the Controller and the Data Subject, or necessary at the request of the Data Subject prior to entering into a contract.
- **Legal Obligation**: the processing is necessary for compliance with a legal obligation to which the Controller is subject (e.g. a nonprofit might be obliged to notify Tusla where they become aware of allegations of child abuse).
- **Vital Interests**: the processing of the personal data is necessary in order to protect the vital interests of the Data Subject.
- **Public Interest / Official Authority**: the processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official, regulatory or statutory authority, which is vested in the Controller (e.g. where the nonprofit is acting as an agent for the Department of Social Protection, or the HSE, in providing a service).
- **Legitimate Interest**: the processing is necessary for the purposes of the legitimate interests pursued by the Controller or the Processor, except where these are overridden by the interests or fundamental rights and freedoms of the Data Subject, particularly where he or she is a child.

Lawful Processing Conditions – Special Categories of Processing

Special categories of processing (processing of medical information, or information relating to race, religion, political beliefs, etc.), receive an additional level of protection under the GDPR. Such processing must be justifiable with reference to at least one condition from Article 9 of the Regulation – if this cannot be done, then the organisation should not be processing such information. For example, when processing these special categories of personal data, the consent of the Data Subject needs to be explicit and cannot be implied or assumed.

The full list of Conditions from Article 9 is as follows:

- The Data Subject has given ***explicit consent*** to the processing of those personal data for one or more specified purposes; or
- The processing is necessary for the purposes of carrying out the obligations of the Controller or of the Data Subject in the field of ***employment and social security and social protection***; or
- The processing is necessary to protect the ***vital interests of the Data Subject or of another person*** where the Data Subject is physically or legally incapable of giving consent; or
- The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other ***non-profit-seeking body*** with a political, philosophical, religious or trade-union aim, in connection with its ethos and purposes; or
- The processing relates to personal data which are ***manifestly made public*** by the Data Subject; or
- The processing is necessary for the ***establishment, exercise or defence of legal claims*** or whenever courts are acting in their judicial capacity; or
- The processing is necessary for reasons of ***substantial public interest***; or
- The processing is necessary for the purposes of ***preventive or occupational medicine***, 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 pursuant to contract with a health professional; or
- The processing is necessary for reasons of public interest in the area of ***public health***, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; or
- The processing is necessary for ***archiving purposes in the public interest***, or scientific and historical research purposes or statistical purposes in accordance with the Regulation.

Top Ten Tips - Recommendations when preparing for the GDPR

By way of summary, we recommend that nonprofits start their journey towards GDPR compliance with the following ten tips (please read these suggestions in connection with the rest of the document):

1. **Assess your current data management status and become accountable**: in the course of an internal assessment, which involves every department of the organisation, identify all types of data processing activities by checking:
    - Which personal data was obtained from which Data Subject?
    - On what basis was the data sought, and using what level of consent?
    - For what purpose or purposes was such data obtained?
    - Did any excessive and unnecessary processing occur since? Has the data been kept accurate and up to date?
    - How long will the data be retained?
    - Are Data Processors (third party service providers) involved in the processing?
    - Do the Data Processors know of the retention period and contractual obligations?
    - Is the data safe and secure? Have we implemented adequate organisational and technical measures?
    - Who can access the data and where and how is it stored?
    - Is it encrypted or pseudonymised?
    - How will it be shared and which type of data processing agreements are in place?
    - Are international protection mechanisms necessary, and if so, are they in place?
    - Safeguarding of children and vulnerable persons: Garda vetting requirements for volunteers, employees, etc.
    - Compliance with Anti-Money Laundering legislation: What protocols are followed when large cash donations are received from an unverified or suspicious source?
    - Appropriate use of PPSN for reclaiming tax for charitable bequests from Revenue Commissioners
    - Mandatory data sharing or disclosure requirements to Public bodies as required by specific Legislative requirements i.e. mandatory HSE or Tusla disclosure requirements.*

*__Note:__ The Office of the DP Commissioner gets a lot of queries on this topic alone.
Where a data disclosure request comes in from a Public Sector body, e.g. "We need to see all of your customers' data on who received a service in 2017", or "Please provide us with a list of all of your employees' salaries", then this request has to be lawfully justified by the Public Sector body prior to any data disclosure.

In responding, the Public Sector Body should be able to identify the specific section of the appropriate Act that requires such disclosure. As Data Controllers, Charities would need to individually assess any such disclosure requests to ensure that they are legally justified and appropriate. Disclosing personal data of customers or service recipients on the basis that funding will be stopped by the Public body should never be a reason for the automatic or unchallenged disclosure of personal data.

2. **Establish the legal basis and consent:** for nonprofit organisations in particular, establishing a solid database, which meets at least one of the lawful processing conditions, is vital for its ongoing campaigns, communications and fundraising activities. All lawful processing conditions need to be defined and corresponding consents need to be recorded. Communication preferences have to be noted on the client or donor database. Under the GDPR, organisations will be required to show evidence of how the data was acquired, and the legal basis for which it was acquired. Where necessary, a quality review exercise may have to be conducted in order to 'firm up' the data quality (for example, Sytorus uses a tool called a 'Principle 4 Campaign' in order to carry this out. See section entitled *Quality Review Exercise – A 'Principle 4 Campaign'* below). Particular attention needs to be given to the consent acquired for processing of data relating to children and to special categories of processing.

3. **Differentiate processing activities**: in line with its Lawful Processing Conditions and any consent recorded in this regard, nonprofits should ensure that any communication and marketing activities are clearly differentiated according to purpose. For example, a clear delineation needs to be drawn between servicing communications relating to the services being offered by the organisation (for example, the acknowledgement sent to a donor when they have made a donation) and marketing or fundraising messages intended to raise awareness and raise donations. One set of communications should not 'bleed into' the other without setting the appropriate expectations with the recipients.

4. **Subject Access Requests and other Rights:** nonprofits need to adequately prepare for such requests and ensure that all rights and freedoms of Data Subjects are sufficiently protected.

5. **Data Protection Officer:** a Data Protection Officer (DPO) needs to be appointed by law in certain circumstances, but it is recommended best practice to appoint such a role in any organisation which processes special categories of personal data. This is not a 'stand-alone' role, and can be added to the responsibilities of an existing staff member.

   Furthermore, the GDPR permits several organisations to collaborate and 'share' a single Data Protection Officer. This is something that should be considered by a group of nonprofit organisations operating in the same area or which provide a similar service.

6. **Processing Logs**: all data processing activities need to be logged in a transparent and auditable manner in a tracking system or spreadsheet. It is recommended that the Data Protection Officer, where appointed, takes overall responsibility for managing such a system. This is crucial for complying with the evidence-based approach, which will be set in place by the GDPR, as unannounced audits from the Office of the Data Protection Commissioner are possible any time after May 2018.

7. **Detecting and Reporting Data Breaches**: suitable internal reporting structures must be in place to ensure that all staff find, report and investigate breaches in accordance with the law and, in turn, notify the Office of the Data Protection Commissioner and the Data Subject where necessary. Such breaches and the way they were dealt with need to be logged. This reporting activity can be the responsibility of the Data Protection Officer.

8. **Privacy Impact Assessments**: the organisation needs to apply the 'Privacy by Design and Default' principle into its operations and carry out Privacy Impact Assessments on a

regular basis, where this is required by law. In brief, the GDPR requires that, where any proposed change to a system or operational process introduces risk to the processing of personal data, the organisation must conduct a risk assessment and design appropriate measures to mitigate or reduce the impact of these perceived risks. Cooperation with the Office of the Data Protection Commissioner may be required.

9. **International Transfers**: where transfers to organisations in non-EU countries take place, organisations need to ensure that suitable security safeguards are in place – including audits, contractual terms or processing conditions.

10. **Supervisory Authorities and Regulatory Bodies**: each EU jurisdiction will have an authorised body for ensuring compliance with the GDPR. Irish nonprofits / the Irish community, voluntary and charity sector will most likely report to the Irish Office of the Data Protection Commissioner, but need to keep abreast with developments as the role of 'Supervisory Authorities' will be clarified in the near future as well guidance coming from the office of the Irish Charities Regulator and other official bodies

    Irish Charities Regulator requirements (http://charitiesregulatoryauthority.ie/)

Consent - Current Law

In preparation for the GDPR, organisations are advised to check the quality of the personal data they hold, and the quality of consent for direct marketing purposes in particular. One of the primary sources of complaints with the Office of the Irish Data Protection Commissioner is the lack of clear consent for electronic direct marketing, i.e. the recipient of a promotional message disputing the fact that they ever gave consent, or claiming that they had declined to give consent and were nonetheless contacted.

Aside from using data for Direct Marketing purposes, many nonprofits rely on the consent of their service users on a day-to-day basis. It is important, therefore, that this consent is freely given and that the implications of giving consent are clearly understood by the Data Subject.

In the context of Direct Marketing, the current legislation differentiates between new and existing customers or donors when it comes to consent:

New Customers or Donors	**Existing Customers or Donors**
Post: No prior consent required, but all promotional messages must offer the recipient a free and easy-to-use option to opt out from receiving further messages.	**Post:** No prior consent is required, as long as the individual was given the option to opt out at the time their data was acquired. All promotional messages must offer the recipient a free and easy-to-use option to opt out from receiving further messages.
SMS messages and e-mail: Explicit prior consent is required to use personal contact details for marketing purposes; where consent is received, use the data for that purpose at least once in each 12-month period; and each message must remind the recipient that they have a free and easy-to-use option to opt out from receiving further messages.	**SMS messages and e-mail:** Explicit prior consent is required. Where such consent was given, recipient must have had the option to opt out at the time their data was acquired initially, as well as in subsequent marketing messages. Personal data can continue to be used for direct marketing purposes if the data is used for that purpose at least once in each 12-month period from the date it is acquired; and each message must remind the recipient that they have a free and easy-to-use option to opt out from receiving further messages.
Calls to land-line and mobile phones: Prior and explicit consent is required for marketing where the number is listed in the National Directory Database (NDD). Where consent is given, data for that purpose must be used at least once in each 12-month period; and each time the recipient must get a free and easy-to-use option to opt out from receiving further messages. No prior consent is needed where the number is not on the NDD.	**Calls to land-line and mobile phones:** Where such consent was given at acquisition, recipient must have had the option to opt out at the time their data was acquired initially, as well as in subsequent marketing messages. Personal data can continue to be used for direct marketing purposes if the data is used for that purpose at least once in each 12-month period from the date it is acquired; and each message must remind the recipient that they have a free and easy-to-use option to opt out from receiving further messages.

When it comes to direct marketing, the **'double opt-in' principle** applies to all Irish nonprofit organisations. It is *not* sufficient that an individual donates to a particular organisation or

campaign in order for their details to be added to your direct marketing list – *separate, clear consent must be acquired for this purpose*.

Consent Under the GDPR

The GDPR, due to come into force in May 2018, will introduce a new definition of **consent** for all purposes, not just Direct Marketing. Consent will now be any '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' (Article 4.11).

In order to comply with this standard, organisations will need to be able to:

- Explain when and how they acquired the personal data of the Data Subject;
- Explain the purpose or purposes for which the data was acquired;
- Demonstrate the quality of the consent they have received (this requires organisations to keep a record of the interaction with the Data Subject at the point of collecting his or her consent).

These more stringent criteria are likely to raise some challenges for organisations with regard to the consent they have for marketing and other purposes. There is a natural concern that the data they currently hold will not meet these stricter criteria.

The guidance from the Office of the Irish Data Protection Commissioner is that data can only continue to be used for Direct Marketing purposes where the quality of consent can be shown to meet this standard. In this regard, the GDPR states in a recital that processing, which is already under way on 25 May 2018, should be brought into conformity with the Regulation.

This will mean that organisations will need to review the quality of the data they already hold, and ensure that it meets the new consent criteria prior to May, 2018. Otherwise, it may no longer be possible to use consent as the basis for processing the data, and another Lawful Condition will need to be provided for that purpose.

Where processing is based on consent, it is not necessary for the Data Subject to give his or her consent again if the original consent is in line with the conditions of the Regulation. In such circumstances, the Controller can simply continue to use the data as before.

However, where the original consent does not meet these criteria, it may be necessary to conduct a data quality review prior to May 2018, as outlined below.

Consent - Preparing for the GDPR

In preparation for the GDPR, we recommend that organisations take the following steps:

1. Review the current list of personal data which is intended for use in direct marketing campaigns;
2. Assess the quality of the consent acquired from these individuals against the criteria provided above.

Secondly, on the basis of these assessments, organisations can classify their data into three categories: Gold, Silver and Bronze.

'Gold Standard'	**'Silver Standard'**	**'Bronze Standard'**
This applies to those sets of personal data which meet the acceptable criteria of the GDPR, and there is confidence that the individual continues to support the organisation.	Personal data does not meet the stringent GDPR criteria. Records may be missing, no consent was actively sought or the data was not used in the most recent 12-month period.	There is no confidence regarding the manner in which the data was acquired, and no evidence that there has been any interaction or response from the individuals during previous campaigns.
This database will instantly form the core distribution list for future direct marketing campaigns.	Further work is required in order to bring this data up to the required standard. A quality review exercise is recommended. (See below)	The organisation should consider removing this data altogether, on the basis that sanctions and damage to the brand will likely outweigh the benefits of any campaign.
Risk level: Low. A complaint is unlikely.	Risk level: Medium. A complaint may occur, a defense to this complaint may be inadequate, and further work needs to be done.	Risk level: High. A complaint about unsolicited marketing is likely, and any defense to this complaint is likely to be inadequate.

Consent Quality Review Exercise - *"Principle 4 Campaign"*

The 'Principle 4 Campaign' is a Sytorus term for a quality review (carried out on the basis of the 'Accuracy' Principle of the GDPR) to:

- **Accuracy**: Establish accurate records of personal details; and
- **Currency (up-to-date)**: Ensure that all contact details are up-to-date.

A quality review exercise of this nature should be carried out where there is uncertainty over the quality of consent given previously ('Silver' data, as above). Where certainty already exists, subjects do not need to be contacted in this way.

When carried out correctly, the 'Principle 4 Campaign' may also allow the Controller to:

- **Product and Service preferences**: Verify the individual's current status and preferences with regard to the organisation's products and services; and
- **Direct Marketing preferences**: Understand and update, where necessary, the individual's preferences with regard to electronic or postal direct marketing.

Please Note: The 'Principle 4 Campaign' must be conducted as a data quality exercise – it would be a direct breach of the Legislation to include ANY marketing aspect or content in this dialogue with the client. It must be the organisation's intention to use the campaign solely to enhance the quality of the personal data already held, and to gain confidence regarding the quality and accuracy of that data.

In a third step, applying clean data management procedures will ensure that those Data Subjects who indicate their consent to be contacted for marketing purposes can be added to the 'Gold Standard' listing.

Those who exercise their right to 'opt out' and indicate they no longer wish to be contacted should be marked as "Do Not Contact" (DNC) for marketing purposes, and should only be retained further by the organisation if there is an appropriate operational or contractual reason to do so.

We strongly recommend that, once this exercise is completed, the organisation maintains a single, consistent list of its clients/donors which is updated regularly and provides an accurate view of customer preferences.

Finally, the organisation must review its registration and client/donor interaction forms (competitions, registration forms, web-site query facility, etc.) to ensure that, from this point forward, any personal data acquired from Data Subjects offers the appropriate options to actively opt in, or to opt out and decline future marketing contact.

Data Subject Rights and Freedoms

Besides the Seven Principles above, the GDPR strengthens existing rights and freedoms of the Data Subject and introduces new rights and freedoms. The Data Subject is any living individual to whom the personal data relates.

These new rights and freedoms are:

- **Right to be Forgotten**: this right to erasure of personal data allows the Data Subject to request from the Controller the deletion of personal data, without undue delay, on particular grounds. In particular, this right is important for nonprofits where they may have collected personal data from a child in the past and where, as an adult, the Data Subject now has a different viewpoint of the risks involved in the processing. (Note that the general age of consent under the GDPR is 16 years and Ireland has introduced a national threshold of 13 years);
- **Right to Restriction of Processing**: in certain circumstances, the Data Subject can request the Controller to restrict processing either permanently or temporarily. For example, the accuracy of data may be contested, there may be concerns that the processing may be unlawful or there are queries over the legitimate interests of the Controller overriding the rights and freedoms of the Data Subject. In the nonprofits, for example, a Data Subject could ask the Controller not to publish a photograph from a fundraising event showing his or her face until the lawful processing condition for this is clarified.
- **Right to Object to Certain Processing**: the Data Subject is entitled to object to the processing of their personal data based on his or her situation, preference or state of mind. Where data is processed, for example, for the purpose of direct marketing, consent may be withdrawn at any time and free of charge. An objection to processing may be overridden in certain circumstances. For example, Irish law may require the Controller to continue keeping fundraising records for financial auditing reasons. However, the organisation has to bear in mind that the burden of complying with such an overriding factor rests with the Controller, not the Data Subject.
- **Right to Data Portability**: where a Data Subject is moving their account from one provider to another (or one organisation to another), the Data Subject should be able to receive a copy of his or her personal data in a structured, commonly used, machine-readable format. There are some exceptions to this right.
- **Right of Access to Information**: where the Data Subject submits a written request, the Controller must provide a copy of any information relating to the Data Subject without undue delay and at the latest, within one month of receipt of the request. Any reference to other individuals in the data must be removed or redacted before the information is handed over. This deadline may be extended to two months in certain situations. There will be no fee for this facility under the GDPR, unlike currently where a maximum fee of €6.35 applies.
- **Right to Complain, Right to Judicial Remedy**: where a Data Subject is not satisfied that the Controller adhered to its obligations under the GDPR, he or she can consider bringing a complaint to the Irish Data Protection Commissioner or seek a judicial remedy in the Irish courts.

Profiling and Automated Decisions

Under the GDPR, the Data Subject will enjoy certain rights where they are profiled, or where automated decision-making takes place using their personal data. As these are important topics for the Irish community, voluntary and charity sector specifically, they are given greater attention in this guidance manual.

The word 'profiling' is understood in everyday life as a type of analysis of a person's characteristics and information in order to assess and predict their behaviour, preferences or capabilities. Often, it leads to the categorisation of Data Subjects into different groupings or data-sets. In most cases, profiling is done without the individual's knowledge.

The GDPR, by contrast, defines processing as an automated activity. **Profiling** is 'any form of *automated processing* of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person'. Given examples relate to an individual's likely behaviour, their reliability based on past performance, as well as their interests and personal preferences.

Where a nonprofit organisation uses an automated system or application in order to categorise personal data into groups of people who are likely to be interested in this campaign or that campaign, this is profiling as defined by the GDPR.

Using today's technological capabilities, organisations can determine, analyse and predict people's interests and habits to sophisticated standards and often without them realising fully the extent of the analysis that is being carried out. This contravenes the Principle that processing needs to be done in a fair and transparent manner (Principle 1).

As a result, Data Controllers need to assess and evaluate their profiling activities according to the Seven Principles above. For example, they need to:

- **Fair, lawful and transparent:** give full and easy-to-understand information on their processes and establish lawful processing conditions in relation to profiling.
- **Specified and Lawful Purpose**: define a specific purpose for the profiling, rather than leaving such activities open-ended or indiscriminate.
- **Minimisation:** ensure that the minimum amount of personal data is acquired and used in the course of a profiling activity; restrict visibility to data in the course of profiling by applying pseudonymisation techniques.
- **Accurate and up-to-date:** put regular checks in place to ensure the accuracy of the data used and that, as far as possible, all preferences of the Data Subject are up to date.
- **Retention:** define the retention period for which personal data is held in this context and where possible, anonymise data as soon as possible.
- **Safety and security:** implement adequate organisational and technical measures to keep the data safe both in terms of human error as well as IT systems. Train all staff appropriately.
- **Liability:** where other parties are involved in the profiling activity, delineate liability and ensure full transparency.

The GDPR requires further that where a Data Controller makes a decision based solely on automated processing, including profiling, the Data Subject will have the right not to be subject to such a decision. It is important here to note, though, that this only applies where the decision in question produces 'legal effects' or an effect which 'significantly affects' the individual concerned. As ever, exemptions apply.

In summary, nonprofit organisations should heed the consent of the Data Subject as follows:

Profiling	**Decision based on automated processing (this can include profiling) with legal or similar effect**
Prior consent is not necessary, but Data Subject should be able to opt-out at any stage. Full information concerning the profiling activity needs to be provided to the Data Subject at first point of contact.	Prior consent is necessary - the GDPR says that the individual has 'a right not to be subject' to such decisions, so the default is that the Data Subject is offered a choice with regard to such activities.
Example: "*We may tailor our communications with you, including our marketing campaigns, based on analytics we perform on the data you provided to us in the course of (interaction). You may ask not to be included in such analytical operations by contacting our Data Protection Officer (details).*"	Where an individual applies through a nonprofit organisation to be considered for a social welfare entitlement or subsidy, this evaluation might be offered on-line via an automated decision-making process – the individual must be given the option to apply using an alternative means, for example, to speak with a member of staff and have their application considered by a person, rather than solely by the system or automated process.
Any objection will need to be accurately recorded in the database of the organisation and taken into account during any future profiling activity.	Where such a scenario does arise, prior consent needs to be recorded in the database, or an alternative decision-making process needs to be made available

Subject Access Request

The Data Subject will have the right of access to their personal data which was collected concerning him or her and can exercise that right easily and free of charge, in order to be aware of, and verify, the lawfulness of any processing which is being conducted. The organisation must respond within one month of receiving the valid, written request.

Every Data Subject has the right to know, from the Data Controller:

- Who processed their personal data where, when and how;
- Why such data was processed;
- For how long such data was processed;
- The recipients of the personal data;
- Where applicable, the logic involved in automatic processing, including profiling and the consequences of such processing.

In addition, the requestor will be entitled to a copy of any personal information held by the organisation which relates to him or her. Some exemptions apply.

In a nonprofit context, this may be the right to access donation, fundraising and campaign data as well as information on the receipt of services from the organisation. It may also include data concerning profiling and direct marketing. Nonprofits must be prepared for such a request and have a set of procedures in place to deal with this.

Where the personal data might be held by a third party on behalf of the nonprofit (e.g. by a Data Processor), the nonprofit needs to ensure that the Data Processor contract covers any circumstances where the third party will be obliged to assist in responding to a Subject Access Request.

As the Data Controller, the nonprofit must ensure that there is no delay in responding, even where some proportion of the personal data may need to be collected from a third party.

Obligations on Data Controllers

The GDPR will introduce procedural obligations on organisations who are involved in the processing of personal data, in particular, the Data Controller and the Data Processor. Whilst some liability may be apportioned to the Data Processor or another Joint Controller, the Data Controller is the party which is principally responsible for the processing of the data in question.

Key responsibilities will include:

- **Process logging**: every processing activity needs to be recorded in a tracking system, which is maintained on an ongoing basis; adequate, documented reports on such processing activity needs to be available when requested by the Office of the Data Protection Commissioner (unannounced audits are permissible under the GDPR); the log must include such details as the parties involved, the purpose of the processing, the categories of personal data and Data Subjects, the recipients, any transfers outside the European Union, and so forth. As such, the obligation to document a data processing log replaces the current system of registering with the Office of the Data Protection Commissioner. The Processing log becomes a key mechanism to demonstrate compliance in the future. Process Logging only applies to organisations with more than 250 employees, but some smaller organisations, including nonprofit organisations, will also have this obligation where they regularly process sensitive data or conduct special categories of processing.

- **Logging breaches**: any personal data breaches of which the Controller or Processor are aware must be documented, in line with the processing log system described above.

- **Breach notification to the Office of the Data Protection Commissioner:** only breaches which are likely 'to result in a risk for the rights and freedoms of individuals' will need to be reported, but that is a broad definition and the deadline is 72 hours from becoming aware of such an incident. Any delay in reporting, beyond that point, must be explained with a reasonable justification.

- **Breach notification to the Data Subject:** such notification, which must be given 'without undue delay', must be made where the Controller is aware of an incident which exposes the data or the rights and freedoms of the Data Subject to risk. Certain encryption or pseudonymisation techniques may prevent the Controller or Processor from having to notify the Data Subject, e.g. where a device containing personal data is lost or stolen, but the device itself is encrypted, the data is considered safe and no notification to the Data Subjects is necessary.

- **Data Processing Contracts:** the GDPR will require the Controller to enter into a Data Processing Agreement with each Data Processor who is involved in the processing of personal data on the Controller's behalf. This contract needs to be in writing and must cover certain basic requirements, such as guarantees concerning the safety and security of data, auditing rights, cooperation concerning the rights and freedoms of Data Subjects and so forth. A similar written agreement needs to be put in place where the Controller

enters other arrangements, e.g. between two nonprofits in a group hierarchy; between Joint Controllers or where several Processors work together in one processing activity.

- **Sub-contracting**: the Controller needs to be aware that where a Data Processor enlists another processor for carrying out specific processing activities on behalf of the Controller, it will be the responsibility for that Processor to ensure that the same level of protection exists for the data during this element of the processing, as exists between the Controller and the initial Processor. In the community, voluntary and charity sector, an example could be where a data analytics company carries out a profiling activity on a database belonging to a nonprofit, but in turn uses a self-employed consultant who works side-by-side with its in-house employees. In this case, the clauses of the data processing agreement between nonprofit and the analytics company must be mirrored in the data processing agreement between the analytics company and the self-employed consultant.

- **Privacy Impact Assessments**: where a significant change to data processing operations are likely to result in a high risk to the rights and freedoms of the Data Subject, the Data Controller will be required to carry out a Privacy Impact Assessment in order to evaluate the risks inherent in such changes. In particular, attention has to be given to the origin, the nature and the severity of the risk in question.
  The results of this Impact Assessment must be documented and retained, and must be made available to the Office of the DP Commissioner (ODPC) on request. Any identified 'high risk' has to result in the Controller engaging with the ODPC before the processing activity in question begins.

- **Data Protection by Design and Default:** in line with the requirement to carry out a Privacy Impact Assessment, the principles of 'Data Protection by Design' and 'Data Protection by Default' place privacy and the rights and freedoms of the Data Subject at the heart of any current or future processing activity. In a nonprofit context, this can include direct marketing, fundraising, profiling, analytics, outsourcing of services and upgrading of the back office database. It may also capture all data processing activities and how, after writing processing logs, the organisation intends to minimise any processing in question and ensure that no unnecessary actions on personal data are taken.

Data Protection Officer

The Data Protection Officer ('DPO') plays a key role in ensuring that the Data Controller and the Data Processor are compliant with the complex requirements of the GDPR. Under the Regulation, a DPO must be appointed where one of the following criteria applies:

- where the organisation processes data in a manner which requires 'regular and systematic monitoring of Data Subjects on a large scale' ('large scale is not defined');
- where the data processing activities 'consist of processing on a large scale of special categories of data'; or
- where the organisation is a public body or has statutory authority, or processes personal data on behalf of such an organisation.

In our experience, many nonprofit organisations from across the sector regularly process special categories of personal data – data relating to an individual's physical and mental health and well-being, ethnicity, religious beliefs, criminal records, etc.

Even where a mandatory obligation to appoint a DPO may not exist, we recommend that organisations nonetheless consider the training and appointment of a member of staff to be responsible and knowledgeable regarding Data Protection within the organisation (the 'Data Protection Champion'). Ultimately, this can only assist with raising staff awareness, embedding good data management practices, and making an organisation data protection compliant.

Key features of this new role are:

- The DPO or DP Champion can be part-time, but no conflict of interest should impact his or her independence and impartiality when carrying out the role, which is why recommendations were made at European level that persons who take managerial decisions may not be suitable as DPOs (in particular, senior managers in HR, Marketing, Fund-Raising and IT would be considered to have a conflict of interest);
- The DPO may be an existing staff member or the role may be outsourced, but the candidate must demonstrate expert knowledge of the legislation, be sufficiently qualified and experienced, and understand the business model and data processing activities of the organisation in question;
- A direct reporting line to senior management should be established, so that the DPO can clearly report on data processing compliance, notify in the event of incidents and make suitable recommendations;
- The DPO must have sufficient resources available to him or her to do their job;
- The DPO cannot be penalised for his or her decisions, actions and recommendations in certain circumstances, and needs to be supported in an inclusive, collaborative manner.

The DPO will be required to:

- Inform and advise the organisation's management and employees;
- Monitor compliance;
- Assign responsibilities, raise awareness, provide training and conduct internal audits;
- Provide advice where requested and carry out Privacy Impact Assessments;
- Cooperate fully with the Office of the Data Protection Commissioner;
- Act as the contact point for the Commissioner, the authorities, the Data Subject and the public.

Further information will be available to DPOs and organisations in the coming months as the Office of the Data Protection Commissioner, as well as relevant European institutions and bodies, provide greater guidance in respect of this role.

Data Sharing and Overseas Transfers

Flows of personal data to and from Ireland are often obscure in the sector and could involve:

- Using services of third parties who are not in the European Union, such as a data analytics service or cloud hosting provider in the United States of America;
- Sharing personal data with friendly, like-minded nonprofit partners;
- Where an Irish nonprofit organisation belongs to a global network of nonprofits, sharing data within that group;
- An international organisation processing personal data during the course of providing humanitarian services 'in the field'.

The increase of flows of personal data outside the European Union has raised new challenges and the legislators of the GDPR hope to ensure that this does not undermine the rights and freedoms of the Data Subject. Transfers to third countries may only be carried out in full compliance with the GDPR. Transfers may occur:

- Where a country outside the European Union enjoys the status of 'adequacy' (note that the United States of America does not currently enjoy this status – to date, only ten countries world-wide have applied for and received this status);
- Where appropriate safeguards are in place, such as Binding Corporate Rules or Special Contractual Clauses in Model Contracts.

In the case of data transfers to and from the USA, the EU-US Privacy Shield is in place, which requires US companies to comply with certain principles and a defined enforcement regime. This Privacy Shield, together with the other international safeguards, are under constant review on an Irish and European level. DPOs and their respective organisations need to keep a watchful eye on developments in this area.

Where the Data Subject has given explicit consent or the transfer is necessary for specific reasons as defined in the GDPR, the international protection mechanisms do not need to apply. It is therefore important for organisations to check which information about the intended processing was provided to the Data Subject at the point of first contact, and the clarity of consent which was obtained in relation to transfers of personal data overseas.

Supervisory Authorities

Irish nonprofits will report to the Office of the Data Protection Commissioner, the 'Supervisory Authority', as defined by the GDPR.

A noteworthy exception occurs where cross-border processing takes place and the decision concerning such cross-border processing are taken in another country. For example, one office of a nonprofit organisation might be based in Dublin, but its international headquarters, responsible for its data management policy, might be based elsewhere within the EU.

Where such policy decisions are taken in another European country, the Supervisory Authority in that country becomes the 'Lead Supervisory Authority' and takes ownership of the matter, in cooperation with the Irish Commissioner.

Where the decisions are taken in a country which is outside the European Union, the legal entity who takes such a decision needs to appoint a 'nominated representative' inside the European Union, who will in turn report to the Supervisory Authority of the country in which it is processing personal data.

These are complex new developments in the data protection compliance framework and further guidance is expected from the Commissioner and other relevant bodies in the coming months. In the meantime, it is essential for Irish nonprofits to examine their operations to establish whether or not any cross-border processing takes place. As the GDPR embeds in the Irish legal framework, Controllers and Processors need to watch this developing space and keep up to date with new guidance.

Sytorus will continue to monitor these developments, and will expand on this guidance for the sector as soon as it is available.

Top 10 Do's and Don'ts for Nonprofits

DO!	DON'T!
Do carry out an assessment and prepare for the GDPR in a systematic manner on the basis of identified risks. This legislation introduces a wide range of changes to data protection compliance.	Don't leave it to the last minute - your organisation handles more data and in more complex ways than you might think, and it will take time to get ready for the GDPR!
Do appoint a Data Protection Officer or 'Champion' as soon as possible to take ownership of this compliance project.	Don't allow an untidy database to drag down your compliance standards and your good reputation.
Do check your lawful processing conditions, the quality of your consents and recording these consents on your database.	Don't forget to invest in staff training: according to studies, human error accounts for more breaches than cyberattacks or technical malfunctions combined.
Do include all aspects of your organisation in your compliance, as data protection reaches from reception all the way to management.	Don't transfer data to a country outside the EU without adequate safeguards.
Do carry out Privacy Impact Assessments and build 'privacy by design' into all your projects.	Don't process data with others without having an appropriate data processing agreement in place.
Do log your data processing activities in a tailored process logging system or report.	Don't miss the opportunity, where possible, to apportion some element of liability to other entities.
Do prepare for Subject Access Requests, the Right to be Forgotten, the Right to Opt out of Profiling and other Data Subject rights and freedoms.	Don't merge servicing and direct marketing communication into one undefined message.
Do put in place systematic data breach prevention systems and data breach notification systems. Consider both physical measures (locks and CCTV), organisational measures (different authorisation levels for staff) and technological solutions (password protection, back-ups and encryption)	Don't put your head in the sand when a breach occurs - transparently communicate with the Office of the Data Protection Commissioner and the Data Subject, where necessary, to prevent further escalation or recurrence.
Do take part in the wider national debate on data protection in the Irish community, voluntary and charity sector – network with others in your sector, attend conferences, breakfast briefings and other events which can help you stay up to date.	Don't disregard the sanctions and fines of the GDPR, as they can be significant and will apply equally to the nonprofit and 'for profit' sectors.
Do adopt a proactive approach - the more transparent and regulated your processing	Don't forget about brand value – the biggest impact of a data breach is reputational.

activities are the less exposed you are to risk and the more value you get out of daily operations.	Adhering to best practice data protection standards will put your organisation at the forefront of developments and shore up trust and goodwill from your donors, your strategic partners, your service recipients and the general public.

Sytorus are happy to have collaborated with The Wheel in order to provide this guidance document. Sytorus will continue to work with The Wheel by providing training, advisory and consultancy services to member organsations.

If you or your organisation have any further questions, or require clarification on any of the points made in this document, please don't hesitate to contact The Wheel team, via Training and Advice Coordinator, Mairead O'Connor, mairead@wheel.ie.

Disclaimer: This guidance document is to assist Irish nonprofits in their understanding of their duties, it should not be regarded as a legal interpretation of the General Data Protection Regulation, or any other law and does not constitute legal advice. Organisations are recommended to obtain their own professional advice where necessary. The Wheel and Sytorus accept no responsibility or liability for any errors, inaccuracies or omissions in this document.

The Wheel is Ireland's national association of community, voluntary and charitable organisations. We are a representative voice and a supportive resource that offers advice, training, influence and advocacy for the sector.

Sytorus Ltd is one of Ireland's leading providers of data protection training, consultancy and assessment services.

SYTORUS
DATA PROTECTION SPECIALISTS

The Wheel, 48 Fleet Street, Dublin 2

+353 (0) 1 454 8727 | info@wheel.ie | www.w.wheel.ie
Find us on Facebook, Twitter and LinkedIn

Registered Charity No. 20040963
Company No. 302282

the wheel

Stronger Charities.
Stronger Communities.