# Data Protection in the Charity & Voluntary Sector

## Guidelines

**April 2011.Version 5.0**

**Office of the Data Protection Commissioner**

## CONTENTS Page

**INTRODUCTION** 3

**1.** Key Recommendations 4

**2.** Donor Databases 5

**3.** Personal Public Service Number (PPSNs) 9

**4.** Fundraising & Marketing 11

**5.** Data Retention 12

**6.** Security 12

**7.** Third party 'data processors' 13

**8.** Access Requests 14

**9.** Sensitive Data 14

**10.** Data Protection Policies 15

# Introduction

Data protection is essentially all about the protection of the personal data of individuals whether they are customers, employees, donors or clients. Responsibility for ensuring personal data is processed in accordance with data protection legislation[1] lies with the data controller and/or data processor[2].

In 2007, the requirement for not-for-profit charities to register with the Office of the Data Protection Commissioner ceased as a result of amendments to data protection legislation. The Office of the Data Protection Commissioner has since placed an increased focus on the activities within the sector via the Office's audit and compliance functions in order to assess compliance with the Data Protection Acts.

The Office of the Data Protection Commissioner has now conducted a number of audits of charities. On foot of the inspection reports[3] produced as a result of these audits, the Office is issuing this new guidance to all charities. The guidance focuses primarily on the use of personal data collected in conjunction with charities' fundraising activities in order to ensure compliance with the Data Protection Acts 1988 & 2003.

Sections 2-5 of the guidelines offer guidance on specific issues which emerged during audits conducted by the Office. Guidance on compliance with other requirements of the Data Protection Acts is featured in sections 6-10.

The Office of the Data Protection Commissioner also considers that the **'Statement of Guiding Principles for Fundraising'**[4] as produced by the Irish Charities Tax Research Ltd is an extremely comprehensive set of guidelines, with many references throughout to the importance of respecting the privacy of donors and beneficiaries and highlighting requirements around the security of personal data and the need to respect marketing preferences. The Office of the Data Protection Commissioner endorses this guidance as an aid to ensuring best practice and compliant standards across a range of platforms.

---

[1] http://www.dataprotection.ie/docs/LAW_ON_DATA_PROTECTION/795.htm

[2] http://www.dataprotection.ie/docs/Are_you_a_Data_Controller?/43.htm

[3] [The inspection reports themselves remain confidential between the audited organisations and the Office of the Data Protection Commissioner, although the Commissioner reserves the right to comment on any aspect of the audits in the Annual Report. Equally, the charity audited can decide to make the audit report public or share the contents within the sector which it operates].

[4] http://www.charitytaxreform.com/files/R2.%20Guiding%20Principles%20of%20Fundraising%20-%20Feb%202008.pdf

# Key Recommendations

- Information must be fairly collected and all donors must be provided with adequate notice of how their personal data will be processed.

- If a charity has information about people and wishes to use it for a new purpose, the charity is obliged to give an option to individuals to indicate whether or not they wish their information to be used for the new purpose.

- Only the minimum necessary personal data should be sought by charities.

- The retention of PPSNs by charities other than in relation to donations where relief is still owed is a breach of the Data Protection Acts 1988 & 2003.

- Charities should implement a comprehensive retention policy for all records containing the personal data of donors, beneficiaries, registered campaigners etc.

- All marketing preferences should be accurately recorded and respected.

- Every charity should have a security policy and set of procedures which explicitly address the security aspects of any personal data held by the charity or any personal data disclosed to third parties.

- All charities should ensure that donors, clients, service users and employees are clearly informed of their rights under the Data Protection Acts to gain access to a copy of their personal data.

- Every charity should draw up a Data Protection Privacy Policy and a separate Data Protection Statement for its website.

# 1. Donor Databases

Donors and volunteers are the lifeblood of all charities and the Office of the Data Protection Commissioner acknowledges their importance and the care that is taken by charities to manage and sustain these personal relationships, on a lifelong basis in some cases.

A fundamental principle of data protection is 'fair obtaining and processing'.

> "the data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly"
>
> - section 2(1)(a) of the Data Protection Acts 1988 & 2003

'Fair Obtaining' means that an organisation collecting personal data must collect and use the information fairly. This provision requires that at the time of providing personal information, individuals are made fully aware of:

- the identity of the persons who are collecting it (though this may often be implied)
- to what use the information will be put
- the persons or category of persons to whom the information will be disclosed.

Secondary or future uses, which might not be obvious to individuals, should be brought to their attention at the time of obtaining personal data. Individuals should be given the option of saying whether or not they wish their information to be used in these other ways.

If a charity has information about people and wishes to use it for a new purpose (which was not disclosed and perhaps not even contemplated at the time the information was collected), the charity is obliged to give an option to individuals to indicate whether or not they wish their information to be used for the new purpose.

A key finding arising from the series of audits conducted by the Office of the Data Protection Commissioner, concerned the recording of donations received from a whole range of sources into a single donor database, thus allowing the charity to potentially aggregate and match all charitable donations made by individuals.

In many charities it appeared to be the practice that donor details, whether collected on the street, by phone, via post or through a website were being checked against the charity's donor database in case the person was an existing donor. Practices observed included the searching of donor databases for bank account numbers as recorded on giro stubbs or names on cheques being searched in order to ascertain whether these

details matched with donor data already captured as a result of previous donations. If a match was found, any additional details from the latest donation were added e.g. bank account details added to an entry that previously contained a donor's credit card details. In the event of a non-match, a new donor profile was created with details of the donation recorded and a donor id allocated.

The justifications put forward by charities for such practices were:

- Charities needed to capture the details of each and every donor in order that the maximum tax relief could be claimed by a charity if the donor passed the qualifying threshold over a given tax year.

- Charities indicated they wanted to maintain a record of every donation and link each donation to donors in order to have a complete record of all donations received, to create accurate donor profiles and to plan fundraising activities and strategies going forward.

- Charities also maintained that donors wanted the charities to keep a record of all the donations a specific individual makes so that the charity could acknowledge the donor's generosity or determine that donors classified as 'regular givers' should not be included in an upcoming campaign or appeal.

The Office of the Data Protection Commissioner found several donor databases containing the details of hundreds of thousands of individuals. The Office considered that this indicates a worrying lack of knowledge or awareness of data protection principles.

As outlined above, one of the fundamental principles of data protection - 'fair processing' - is whether personal data can be deemed to have been fairly obtained. The recording of a donation or the matching back to an individual in the context outlined above is not viewed as having been fairly obtained by the Office of the Data Protection Commissioner, unless the donor has been made aware that this will happen in advance and has been given the opportunity to opt out. All charities are advised that all donors must be provided with adequate notice of how their personal data will be processed and an opportunity to 'opt-out' from having their data entered onto any charity's donor database.

A message along the lines of the text below could state

> "Your donation will be recorded for audit purposes and retained on X charity's donor database - if you do not wish to have your details stored on our donor database - please tick here

Charities in response, informed the Office of the Data Protection Commissioner that they must record details of all donation transactions for audit and customer relationship management in case donors contact them to query their total donations. The Office of the Data Protection

Commissioner remains to be convinced that there is a justification to store personal data in such circumstances but accepts that charities need to keep records for a brief period for audit purposes. During this time they should not be used for any other purpose. An arrangement such as this would allow a charity to store such details for audit purposes for a defined period and then the details of the donor can be permanently deleted. Donors who opt-out from having their donation recorded and stored on the donor database of a charity could have their donation details temporarily stored in a separate repository for audit purposes if this is considered necessary.

Another fundamental principle of the Data Protection Acts is the requirement that only the minimum necessary personal data should be sought and this should only be used to allow for the performance of the function to which it relates. This requires a charity in all situations to be certain that the data that is being sought is appropriate to the reason for which it was sought. A charity must be able to show that each piece of personal data sought from a person is needed for a legitimate reason.

**Donations received Online**

In an online environment, there is a clear opportunity to capture the consent of an individual to have their donation recorded for tax relief and other stated purposes. Alternatively, the charity can provide an opt-out to allow them not to have their donation recorded at all. Notice of whatever the practice of the charity is with regard to the recording of donations should be made available to the donor up-front.

- The Office of the Data Protection Commissioner advises charities that if an individual is making a credit or laser card donation online they should be provided with notice to the effect that their details will be entered onto the charity's donor database, if this is the practice of the charity concerned.

- An opportunity should be provided for the donor to opt-out from having their details recorded on the donor database. In this way once payment reconciliation and auditing requirements have been met, the details would no longer be retained by the charity.

**Donations received over the Phone**

For credit or laser card donations made over the phone, the Office considers there is a clear opportunity to capture the consent of an individual to have the donation recorded for tax relief purposes or other stated purposes. Alternatively, the charity could provide an opt-out at the end of the call to allow them not to have their donation recorded on the donor database or in a follow up letter to the phone call.

- The Office of the Data Protection Commissioner advises charities that if an individual is making a credit or laser card donation over

the phone they should be provided with notice to the effect that their details will be recorded onto the charity's donor database, if this is the practice of the charity concerned.

- An opportunity should be provided for the donor to opt-out from having their details recorded (aside from meeting payment reconciliations requirements which are normally handled by a third party intermediary). Credit card numbers or laser card details should not be stored in donor databases unless necessary for ongoing direct debit purposes.

**Donations via cheques in the post or to special appeal bank accounts**

The audits conducted by the Office of the Data Protection Commissioner brought to light a practice whereby a donor who makes donations via cheques in the post or donates to special 'appeal' bank accounts is checked against a centralised donor database and if a match is achieved any additional details from the latest donation are added e.g. bank account details are added to an entry that previously contained a donor's credit card details. In the event of a non-match, a new donor profile is created, details of the donation recorded and a donor id allocated.

In the case of 'one off' donations such as lodgements to special appeal funds or cheques sent in with just the cheque book owner's name and bank account (no address), the charity must not record the details of these donations and use them for another purpose – such as tax relief calculation or user profiling purposes - where there is no consent to do so.

In reaching its conclusions with regard to the legitimacy of recording 'anonymous' donations set against the requirements of the Data Protection Acts, the Office is also cognisant of the 'Statement of Guiding Principles for Fundraising' drawn up by the Irish Charities Tax Research Ltd

> " where anonymity is requested by a donor this will be respected if the donation is accepted, however the other details of the gift will be recorded and published (such that anonymity is preserved), p.16[5]."

- The Office of the Data Protection Commissioner advises charities that in the case of 'anonymous' donations such as lodgements to special appeal funds or cheques sent in with just the cheque book owner's name and bank account (no address), charities must not record the details of these donations and use them for another

---

5 http://www.charitytaxreform.com/files/R2.%20Guiding%20Principles%20of%20Fundraising%20-%20Feb%202008.pdf

purpose such as tax relief calculation purposes or to create a donor profile.

**Donations made by Direct Debit**

- It is recommended that Direct Debit Forms are amended where needed, to highlight the tax calculation purpose. Direct debit donors should be provided with the opportunity to opt-out from having their donation recorded on the donor database

**Date of Birth**

- With regard to the recording of date of birth, capturing the date of birth of donors is not justifiable. It is recommended that the date of birth field is only captured or recorded in circumstances where absolutely necessary, such as a volunteer who signs up to go on a fundraising trek. Age 'ranges' of donors are more than sufficient in assisting a charity with profiling activities. This advice is issued to charities in line with section 2(1)(c)(iii) of the Data Protection Acts 1988 & 2003 which state that

  > "The data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed"

**Donations from Minors**

- Charities should not record the individual details of donors known to be under 18 onto any centralised 'donor' database. The date of birth field should be removed from donor databases and a category to signify 'minor' created if that is deemed necessary for particular campaigns.

## 2. Personal Public Service Numbers (PPSNs)

The Office of the Data Protection Commissioner is aware that Section 848A of the Taxes Consolidation Act 1997 (TCA 1997) provides for a scheme of tax relief for certain "eligible charities" and other "approved bodies" in respect of donations received on or after 6 April 2001. This scheme is administered by the Charity Claims Unit in the Office of the Revenue Commissioners.

In order for a charity to receive this tax relief from Revenue, a charity requires its donors who are PAYE taxpayers and who have donated over €250 euro in one year to complete "an appropriate certificate" supplied to them by the charity. The completion of this certificate includes the provision of their Personal Public Service Number (PPSN) to the charity

and clarification as to whether they pay PAYE at the standard or higher tax rate. The charity can then make an application for tax relief to the Revenue Commissioners by providing an annual set of returns containing the names, addresses, total amount contributed and the PPSNs of all eligible donors who exceeded the donation threshold within a given tax year.

The Office of the Data Protection Commissioner acknowledges that this tax relief scheme has a specific legal basis but retains a fundamental concern that PPSNs collected and retained by charities for tax relief purposes are being integrated onto the charities' 'donor databases'. This practice first came to light in 2008 during the course of an audit of a charity and the charity was immediately instructed to discontinue this practice as part of the audit findings and recommendations.

The Office of the Data Protection Commissioner advises that the retention of the PPSN other than in relation to donations where relief is still owed is a breach of the Data Protection Acts 1988 & 2003.

The Office of the Data Protection Commissioner also advises that it is a criminal offence under the provisions of the Social Welfare (Consolidation) Act 2005 to utilise and retain the PPSN outside of a narrow set of prescribed and limited criteria. Charities do not qualify as specified bodies as set out in the Social Welfare (Consolidation) Act 2005 and therefore the sole legal basis under which they can process PPSNs is under the confines of Section 848A of the Taxes Consolidation Act 1997 (TCA 1997).

In 2010, the Office of the Data Protection Commissioner was contacted by members of the public with regard to a charity who had pre-populated tax relief forms with the PPSNs of its donors. These forms were subsequently issued by the charities to donors seeking their signatures and confirmation with regard to donations made in a given tax year. The Office decided to audit this charity and found that donor PPSNs were also being recorded onto a centralised donor database and the PPSNs were visible to all users granted access to the database i.e. unencrypted.

It is a matter of extreme concern to the Office of the Data Protection Commissioner that PPSNs would form an ongoing part of individual profiles on the donor databases maintained by some charitable organisations. The potential of the PPSN as a unique identifier for donor calculation and profile purposes is a threat to the overall integrity of the PPSN. In addition, the retention of PPSNs undoubtedly increases the risk of abuse of PPSNs and affects the protection and security of individual PPSNs.

The Office of the Data Protection Commissioner is anxious to ensure the use and disclosure of the PPSN is confined to a limited, specific set of circumstances and accompanied by a clear legal basis at all times. It is recommended that

- Certificates being sent to donors by charities for completion should not feature PPSNs pre-populated on the certificate.

- Charities should only capture and retain the PPSNs of qualifying donors for the current tax year.

- The PPSNs of donors collected should be held securely and masked or encrypted. 'Restricted Access' policies should be put in place, confining the number of employees with access to the PPSNs on a strictly 'need to know' basis.

- Once the returns are made to Revenue and the charity receives the relief due, the restricted-access PPSNs should be retained for no longer than necessary, taking into account Revenue auditing requirements.

- The text for donations online or script for donations made over the phone should ask donors whether they are PAYE or self-assessed and whether the details of their donation may be recorded for tax calculation purposes. Equally, the Office of the Data Protection Commissioner recommends that the Data Protection Policy and/or Privacy Statement of each charity is amended to highlight the tax calculation purpose also and the practice governing the restricted use and collection of PPSNs.

# 3. Fundraising & Marketing

Overall, the Office of the Data Protection Commissioner found that a high degree of compliance was in evidence in the sector with regard to direct marketing. Clear evidence that the preferences of individuals were actively respected at all times was observed. Charities sought to capture the consent of individuals to be marketed (or not) from the outset of the relationship with a donor. Also, the charities demonstrated clarity and transparency with regard to the channels through which an individual might be contacted and this is to be commended.

As general advice for the sector, the Office of the Data Protection Commissioner recommends

- Consistency with regard to marketing opt-ins and opt-outs should be applied across all channels taking into account the specific legal requirements with regard to electronic communications because unsolicited electronic marketing is a criminal offence. For example, all e-mail and sms messages should contain an 'unsubscribe' opt-out at the bottom of each e-mail message.

- It is recommended that individuals who have signed up to be kept alerted regarding the progress of various campaigns or new campaigns are not considered fundraising targets unless they have explicitly 'opted in' to receive such communications as well. Equally, donors who support fundraising campaigns should be offered a choice with regard to receiving information on non-fundraising campaigns (sign petitions, postcards etc.)

- The distinction between 'fundraising' and 'campaigning' should be maintained in any type of combined 'supporters' database.

For more detailed information see also 'Direct Marketing'

http://www.dataprotection.ie/docs/DIRECT_MARKETING_-_A_GENERAL_GUIDE_FOR_DATA_CONTROLLERS/905.htm

## 4. Data Retention.

Section 2(1)(c) of the Data Protection Acts 1988 and 2003 provides that a data controller shall not retain personal data longer than is necessary for the purpose or purposes for which it was obtained. It is the responsibility of a data controller to implement a comprehensive retention policy for all records containing the personal data of donors, beneficiaries, registered campaigners, etc.

- A schedule listing all records featuring personal data should be drawn up by each charity containing maximum retention periods for each type of document, file set or database featuring personal data. Non-active donor details should be removed from databases.

- In terms of retention of credit and laser card data, the Office has produced a 'Guidance Note for Data Controllers on Purpose Limitation and Retention in relation to Credit/Debit/Charge card transactions'.[6]

## 5. Security

On the security side, the retention of data gleaned from credit card donations for any function other than payment and reconciliation would not be considered to be in compliance with the Acts. There is no justification for the integration of any details of once-off donors into a donor database other than to document the amount donated and classify the donation as a once-off credit card donation. Any such practices beyond this increase organisational risk in terms of security and the damage that would be incurred if a data breach of donor data

[6] http://www.dataprotection.ie/docs/08/01/08_-_Guidance_Note_for_Data_Controllers_on_Purpose_Lim/581.htm

were to take place by means of a theft or loss of donor data. The same applies to the recording of bank account numbers (except where required for direct debit purposes).

- Where a donation is being made by standing order from a bank account, the bank account details should be stored or held in a masked or encrypted format.

- Removable media: drives and ports should be disabled or restricted unless there is a clear business need to have them available to certain staff.

- All organisational laptops used to process and store personal data should be encrypted and password protected.

- Appropriate user provisioning policies should be in operation governing access rights and the maintenance of these policies, for example 'leavers and movers'.

- Individual user logins should be in use at all times as opposed to generic logins.

- All access to personal data on donor databases should be restricted and subject to monitoring

- Monitoring measures should be made known to staff to discourage inappropriate access.

- In terms of monitoring access on a proactive basis, samples of logs can be checked on a routine basis in order to check for any unusual access patterns.

- In terms of general security advice across all sectors, the Office has produced a guidance note entitled 'Data security Guidance' [7]

## 6. Third party 'data processors'

If a charity uses a third party to process personal data on its behalf for example, a call centre, printing company or IT Service provider then the processing of such data must be covered by contract. The contract should stipulate at least the following:

- the conditions under which data may be processed;
- the minimum security measures that the data processors must have in place;
- some mechanism or provision that will enable the charity (data controller) to ensure that the data processor is compliant with the security requirement. This might include a right of inspection or

[7] http://www.dataprotection.ie/docs/Data_security_guidance/1091.htm

independent audit by the data controller. Guidance on this matter is available at
http://www.dataprotection.ie/docs/7.10_Does_the_Office_of_the_Data_Protection_Commissioner_hav/654.htm

If personal data is being hosted on an external server outside the Irish State, additional legal obligations may apply. See 'Transfers Abroad' - http://www.dataprotection.ie/docs/Transfers_Abroad/37.htm

## 7. Access Requests

Under Section 4 of the Data Protection Acts 1988 & 2003, any individual has the right to request a copy of any data held about them. This applies to all types of information - for example, written details about a person held electronically or on paper, photographs and CCTV images.

An individual is also entitled to know where the information was obtained, how it has been used and if it has been passed on to anyone else.

A person can exercise their rights of access by writing to the charity. They do not need to quote the Data Protection Acts, but the Office of the Data Protection Commissioner would always advise that they do so and include any additional details that would help the charity to locate their information. The charity is entitled to ask for evidence of identity and to charge a fee, but this cannot exceed €6.35.

Once the access request has been made and the appropriate fee paid, the individual must be provided with the information within 40 days (most organisations manage to reply much sooner).

All charities should ensure that donors, clients, service users and employees are clearly informed of their rights under the Data Protection Acts to gain access to a copy of their personal data.

For more detailed information see
http://www.dataprotection.ie/docs/Data_Protection_Rule_8/32.htm

## 8. Sensitive Data

The Data Protection Acts 1988 & 2003 place a particular focus on any sensitive data that may be processed by an organisation.

"sensitive personal data" means personal data as to –

(a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,
(b) whether the data subject is a member of a trade-union,

(c) the physical or mental health or condition or sexual life of the data subject,
(d) the commission or alleged commission of any offence by the data subject, or
(e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

(Section 1. Interpretation and application of Act - Data Protection Acts 1988 & 2003)

Particular care must be taken by charities when processing sensitive data. The Data Protection Acts require additional conditions to be met for the processing of such data to be legitimate. Usually this will be the consent of the person about whom the data relates.

## 9. Data Protection Policies

One key point of contact employed within the charity should be tasked with co-ordinating data protection policy and compliance issues.

- Every charity should draw up a Data Protection Privacy Policy. A Privacy Policy documents an organisation's application of the eight data protection principles to the manner in which it processes data organisation-wide. The policy applies to all personal data processed by the organisation, including customer data, third party data and employee data.

- If the charity has a website in operation, a data protection statement should be drawn up and a link to this statement situated on the homepage of the website. A Privacy Statement is a public declaration of how the organisation applies the data protection principles to data processed on its website. It is a more narrowly focused document than a Privacy Policy.

  For guidance regarding Privacy Policies and Privacy Statements see http://www.dataprotection.ie/docs/PrivStatements/290.htm