FUNDRAISING REGULATOR

PERSONAL INFORMATION AND FUNDRAISING: CONSENT, PURPOSE AND TRANSPARENCY

Produced in partnership with

protecture data protection office

020 3691 5731 | help@protecture.org.uk | www.protecture.org.uk | @protectureDPO

EDITION 1: 21/2/17

Contents

1. Introduction

The Data Protection Act and its associated regulations apply to organisations across the UK. The purpose of this guidance is to help charities and fundraisers better understand their responsibilities in relation to data protection, donor consent and legitimate interests, reflect on their current practices and feel confident in developing a Direct Marketing approach that takes full account of the rights and wishes of the individual.

The Charity Commission in England and Wales, the Scottish Charity Regulator (OSCR) and the Charity Commission in Northern Ireland emphasise the responsibility of charity trustees to ensure fundraising is carried out lawfully and without putting the charity's reputation at risk. As the use of personal data is central to the fundraising activities of many charities, trustees may wish to use this guidance and the issues raised as a basis for assessing risk when holding their organisation's fundraising to account.

The status of this guidance

The Information Commissioner's Office (ICO) is the UK regulator with principal responsibility for upholding information rights in the public interest. The Fundraising Regulator accepts that alternative interpretations of the law on data may be possible in some areas. However, in the absence of case law in these areas, this guidance seeks to present an approach that is consistent with the ICO's interpretation of the law.

The ICO's Privacy Notices Code of Practice, Direct Marketing Guidance and associated guidance and law regarding the use of data should be read alongside this guidance, which is not intended to replace those materials but to provide advice on the practical implications for fundraising. The guidance also takes account of the report of the working group convened by the National Council for Voluntary Organisations (NCVO), which recommended a number of changes to current fundraising practice in relation to the consent of individuals.

Over the summer, we will consider how best to incorporate the key elements of this guidance and the NCVO's recommendations into the Code of Fundraising Practice and we will consult accordingly.

The compliance context

Partly as a result of recent developments – in particular, that the European General Data Protection Regulation (GDPR) will come into full effect in 2018, the NCVO working group's recommendations and the recent civil monetary penalty notices issued to charities by the ICO in relation to what was held to be serious breaches of the Data Protection Act – we believe that there is now a commitment across the sector, in the interests of both donors and beneficiaries, to make consent the primary basis for all fundraising activity and ensure that it is in place wherever it is legally necessary.

Understandably, fundraising organisations want clarity and simple rules to follow to ensure they become or remain compliant with the law. This guidance is designed to be as easy to consult as possible, using the links in the contents page to go directly to particular issues of concern. There is, however, also a duty on each fundraising organisation to interpret and implement the law as they apply to their individual circumstances. The law on data protection and consent is often complex and not every compliance question can be answered with a clear "yes" or "no". As this guidance highlights, charities must consider multiple factors in assessing whether their data practices around personal data are sufficiently robust.

Additional resources

A number of additional resources are available alongside this document at www.fundraisingregulator.org.uk

An **actions checklist** appears at the end of each section. These suggest actions that fundraising organisations should consider in follow up to the issues raised. For ease of use, we have also separated these into a single checklist.

Alongside this guidance, our **consent self-assessment tool** provides a starting point for fundraising organisations to self-assess their circumstances, evaluating the standard of consent they currently operate and the degree of compliance.

Many charities are already reviewing their donor databases to ensure that the necessary consents are place. The **case studies** we have included alongside this guidance provide examples of various ways in which charities are changing their fundraising practices with a view to complying with data protection requirements.

Responding to the challenge

Above all, we need to recognise that legal requirements and compliance, although essential, are only part of the answer. As the NCVO working group's report emphasised, what matters most is charities' commitment to conducting "their fundraising with integrity and respect and, critically, in ways that enable donors to have control". There is a great deal of background noise, again as the working group recognised, about inconsistent guidance, differing views on legal interpretation, and impact on funding and beneficiaries. This is, however, to miss the point – charities must now do the right thing by their donors, aspiring to best practice rather than simply compliance.

To ensure this happens, it is the responsibility of Boards and CEOs to own a set of principles about how their fundraising teams will operate. This includes the central importance of donors and potential donors being in control of their relationships with charities, that personal data should not be exchanged without explicit consent and that consent cannot be presumed to last forever without some process to refresh it.

We would welcome feedback on this guidance. If you have any comments or would like to propose other areas where further information or toolkits would be valuable, please let us know at enquiries@fundraisingregulator.org.uk

Stephen Dunmore
Chief Executive
Fundraising Regulator

2. Glossary of key terms

This section sets out some of the key terms used in this document and how their meaning is defined in the context of the guidance.

Channel

The means of communication between a fundraising organisation and an individual.

Consent

"Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (European Directive 95/46/EC). In the ICO's view, there must be "some form of communication or positive action by which the individual clearly and knowingly indicates their agreement" for consent to be valid (ICO Direct Marketing Guide, 2016). (See also "Opt-in consent", "Opt-out consent").

*For more information, see **Section B** below.*

Data

Information which:

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or

(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)

(Data Protection Act, 1998)

Data controller

A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data matching

The use of old data previously provided by an individual to fill gaps in existing data. For example, use of an individual's old telephone number to find a new one or using an email address to track down their postal address.

*For more information, see **A8**.*

Data Protection Act (DPA)

The Data Protection Act controls how an individual's personal information is used by organisations. Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is used fairly and lawfully.

Data subject

An individual who is the subject of personal data held by the Fundraising Organisation.

Direct Marketing

"The communication (by whatever means)…of any advertising or marketing material…which is **directed to particular individuals**…" (Data Protection Act, 1998). The Information Commissioner's Office states that fundraising activity, as well as the promotional and campaigning activity of charities, is covered by the definition of Direct Marketing (ICO Direct Marketing Guidance, 2016).

The marketing must be directed to particular individuals. In practice, all relevant electronic messages (for example calls, faxes, texts and emails), as well as most addressed mail are directed to someone, so they fall within this definition.

*For more information, see **A3**.*

Fairness and transparency

How an organisation ensures that individuals know about their plans to obtain and use their personal data, and their rights in relation to how their data is used. One of three criteria an organisation must consider before undertaking a direct marketing approach (see also "Purposes", "Lawfulness").

*For more information, see **Section C**.*

Fundraising

Soliciting or otherwise procuring money or other property for charitable purposes. However, any activity that includes the "promotional and campaigning activities of not-for-profit organisations" is covered by Direct Marketing rules (ICO Direct Marketing Guide, 2016).

*For more information on defining the purpose of an activity, see **A.3–A.7**.*

Lawfulness

The legal basis on which an organisation plans to obtain and use personal data. One of three areas an organisation must consider before undertaking a direct marketing approach (see also "Purpose", "Fairness and transparency").

*For more information, see **section B**.*

Legitimate interests

A condition (applicable in limited circumstances) by which an organisation can process personal data on the basis of having legitimate reasons for doing so.

*For more information, see **B.6–B.7**.*

Opt-in consent

An indication from an individual that they agree to receive specified marketing, usually by inviting the person to confirm their agreement by ticking a box. The ICO advise that this is the safest way of demonstrating consent, as it requires a positive choice by the individual to give clear and explicit permission.

*For more information, see **B.8**.*

Opt-out consent

An indication from an individual that they object to or wish to opt out of receiving marketing messages, usually by being invited to tick an opt-out box. The ICO advise that organisations should exercise caution in using this approach as failure to object or opt out only means that the individual has not objected. It does not automatically mean that they have consented.

*For more information, see **B.8**.*

Personal data

Data that relates to a living individual who can be identified –

(a) from that data, or

(b) from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Privacy and Electronic Communications Regulations (PECR)

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act (see above). They give people specific privacy rights in relation to electronic communications. They include rules on marketing calls, emails, texts and faxes.

Processing

Obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data, including –

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data.

(Data Protection Act, 1998)

Purpose

The activities for which an organisation wishes to use personal information. One of three criteria an organisation must consider before undertaking a direct marketing approach. See also "Lawfulness", "Fairness and transparency".

*For more information, see **section A**.*

Privacy Notice

A statement made by an organisation to individuals which discloses how it gathers, uses, discloses, and manages the individual's data. It fulfils a legal requirement to protect a customer or client's privacy.

*For more information, see **section C**.*

Subject access request

A request by an individual to an organisation, exercising their right to access the personal information you collect and hold on them.

Sugging

Selling under the guise of research. If the call or message includes any promotional material, or collects data to use in future marketing exercises, the call or message will be for direct marketing purposes. This applies if an organisation claims it is simply conducting a survey when its real purpose (or one of its purposes) is to sell goods or services, generate leads, or collect data for marketing purposes.

Teleappending

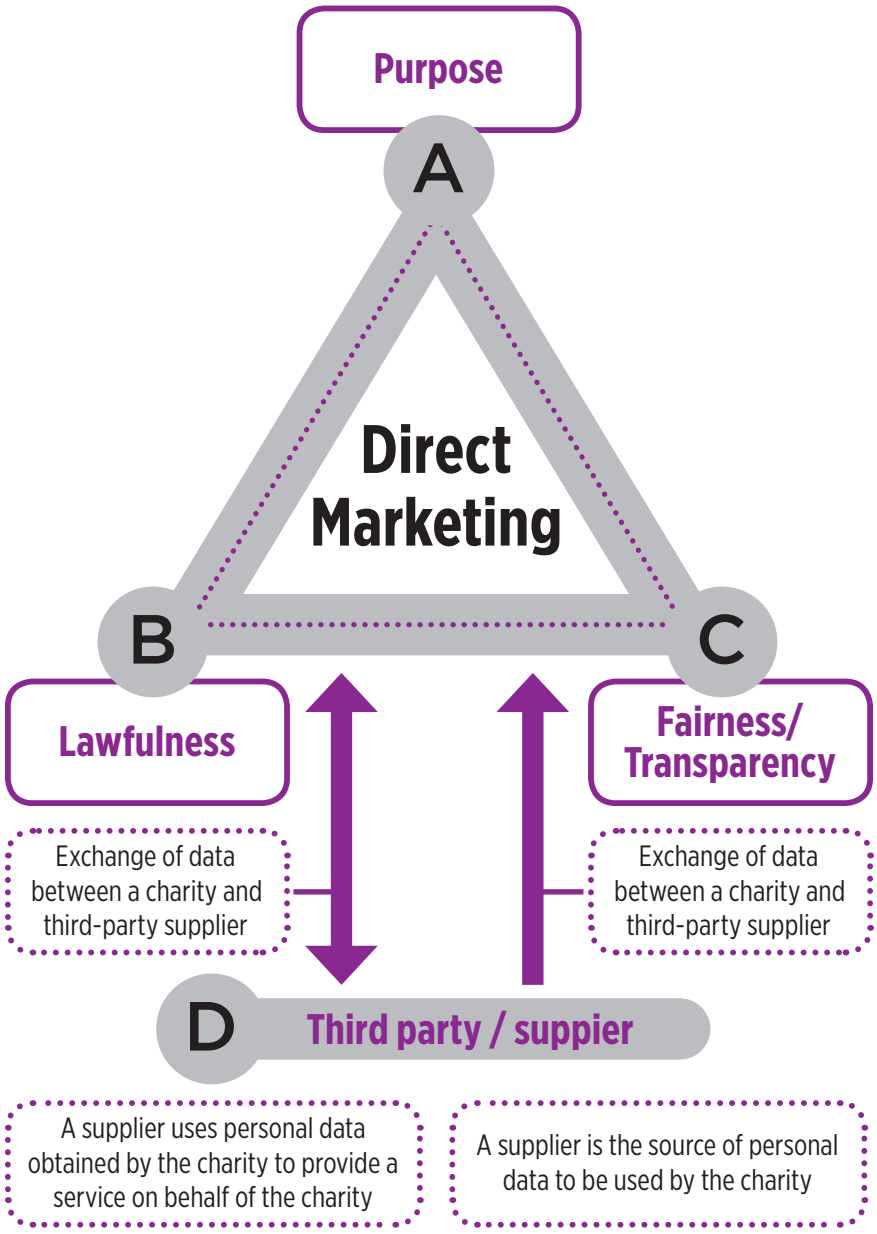
A form of data-matching (see above), focusing on the use of telephone numbers to obtain other personal information.

Wealth Screening

The practice of processing an individual's data for the purpose of profiling them based on their wealth and likely donor value. This may include hiring companies to investigate income, property values, lifestyle, or a person's friendship circles.

*For more information, see **A.3**.*

3. Graphic – Defining your approach to Direct Marketing



Key

Throughout this Guide, the following colour codes are used:

Green:	References to the current Data Protection Act 1998 and Privacy and Electronic Communication (EC Directive) Regulations 2003 (PECR).
Orange:	References to the General Data Protection Regulation (GDPR) due to become law on 25th May 2018.
Blue:	References to existing Codes, Guidance and Case Law.

4. Executive summary

Direct Marketing is defined in the Data Protection Act 1998 (DPA) as

> *…the communication (by whatever means)…of any advertising or marketing material… which is directed to particular individuals.*

The Information Commissioner's Office is clear in its May 2016 Direct Marketing Guidance that 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.

The marketing must be directed to particular individuals. In practice, all relevant electronic messages (for example calls, faxes, texts and emails), as well as most addressed mail are directed to someone, so they fall within this definition.

All charities that undertake, or plan to undertake these activities with particular individuals should therefore define their approach to Direct Marketing to ensure it meets the legal requirements of the DPA and (when using telephone, text or email) the Privacy and Electronic Communication (EC Directive) Regulations 2003 (PECR).

A charity's approach to Direct Marketing should establish

A. What Direct Marketing activities your charity wants to use personal information for (**Purposes**).

B. 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**).

C. How your charity will ensure individuals

   i. are treated fairly;
   ii. know about your proposed use (or uses) of their personal information, and
   iii. can use their rights to manage their personal information (**Fairness and Transparency**).

D. Whether third party suppliers are used and, if so, that these relationships enable your charity to continue to meet its legal and privacy obligations (**Third Party / Suppliers**).

Charities should also assess what impact their approach to Direct Marketing will have on any existing data management systems (for example, Customer Relationship Management (CRM) systems; databases) in order that these systems support the delivery of the agreed approach.

The charity's approach to Direct Marketing should be agreed and reviewed by charity trustees on a regular basis as part of their oversight of fundraising.

5. Defining your approach to Direct Marketing

A: Establishing the purpose (for collecting and using personal data)

This section explains:

- Why it is important to establish your purpose for collecting and using personal data.
- What the law requires and what guidance recommends you do to define your purpose.
- Why it matters if your purpose is Direct Marketing.
- Whether your purpose for undertaking an activity should be defined as Direct Marketing or another purpose, such as administration.

A.1. The importance of purpose

(i) The law relating to Purpose

DPA Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

DPA Part II of Schedule 1, 2(3)(c)

"...the purpose or purposes for which the data are intended to be processed" should be provided to individuals when their personal information is collected.

See **Section C – Fairness and Transparency** *for more information*

GDPR Art. 5(1)(b)

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

Note 1:

Whilst the principle of "purpose limitation" remains similar in both the current DPA and the GDPR, the GDPR adds the requirement that purposes are "explicit."

Note 2: GDPR Recitals 32 and 43

How clearly the purpose(s) for collecting and using personal data are defined affects the standard of consent that can be assumed from the individual. The GDPR says:

- Consent is presumed not to be freely given if it does not allow "separate consent to be given to different personal data processing operations despite it being appropriate in the individual case".
- Consent should cover all processing activities carried out for the same purpose or purposes. "When the processing has multiple purposes, consent should be given for all of them".

See **Section B – Lawfulness** for more information.

Establishing the purpose for collecting and using personal data is one of the key principles of both the current Data Protection Act 1998 (DPA) and the future General Data Protection Regulation (GDPR). Given the range of activities that many charities engage in, it is important for charities to have a clear understanding of the different purposes for which they want to collect and use personal information.

Defining purpose is important because each purpose will determine

- what personal information is needed (for example, which fields of data);
- what the legal basis will be (or what options might be available) that justifies their collection and use of the information, and
- how long the information should be kept.

Defining the purpose will also help ensure that individuals are able to make a fully informed choice about how their data is used. The more precise you can be about this with the individual, the more effectively and confidently you can use any data they have consented to give you.

Privacy Notices, Transparency and Control Code of Practice

Version 1.0.27 07 Oct 2016

"If you empower individuals to manage what you do with their personal data, giving them more choice...you may be able to obtain more useful information from them.

If individuals are able to exercise real choice over what is done with their personal data, you can be more confident that people have provided informed consent for their information to be used...

By taking this approach, you are firstly acting more openly and, in a data protection sense, more fairly, but you are also able to use data more effectively."

Monetary Penalty Notices

December 2016

In December 2016, the ICO issued a penalty notice against two charities for breaches of the Data Protection Act. One area of non-compliance in these cases related to collecting and using personal information for purposes that were not sufficiently explained to individuals.

Charities should consider the benefits of providing individuals with greater choice and clarity regarding the purposes for which they wish their personal information to be used.

A.2. Defining your purpose

Charities should be able to define precisely the purposes for which they want to collect and use personal information. They should distinguish between

1. Direct Marketing purposes (such as fundraising) and other purposes (such as processing a payment or administering staff and volunteers).
2. The different Direct Marketing purposes the charity wishes to use the personal information for.
3. The activities that the charity considers as falling under each Direct Marketing purpose.

For more information on whether your activity is likely to be defined as Direct Marketing or other purposes, see ***Sections A.3.- A.7****.*

Where the purposes are identified as Direct Marketing, charities must consider the extent to which the different types of Direct Marketing activity they wish to undertake are either different to each other (i.e. a different purpose) or similar to each other (i.e. part of the same purpose).

This is explained in the table below.

	Each proposed Direct Marketing activity is	Meaning that	Meaning that	Example
1	distinctly different to other activities	the charity believes each activity is a different purpose.	an individual should be asked to provide separate consent for the charity to use their personal information for each different purpose.	"Fundraising events" might be regarded as a sufficiently different purpose from "campaigning" – meaning that consent should be sought for each of the two purposes.
2	sufficiently similar to each other	the charity believes it can explain and justify why the activities should be covered by a single purpose.	an individual is asked to consent to a purpose – and the charity would use their personal information for all the related activities.	"Fundraising events" might be regarded as a purpose which covers sufficiently similar activities such as the annual dance **and** quarterly runs – meaning that consent for "Fundraising events" would enable the use of the personal information for all related fundraising event activities.

The number of different Direct Marketing purposes and/or activities will vary for each charity, depending on what fundraising activity they undertake. However, charities should be able to explain and justify to those they contact their rationale for decisions about the differences and/or similarities between their fundraising activities (and whether they have consequently determined that separate consents are required or not).

Charities should consider the following advice when considering for what purposes they wish to collect and use personal information.

A.3. Direct Marketing

Direct Marketing is defined in the Data Protection Act 1998 (DPA) as ...the communication (by whatever means)...of any advertising or marketing material...which is directed to particular "individuals". This definition is important for two reasons:

(i) Individuals have a legal right under the DPA to object to Direct Marketing, and

(ii) The definition also applies to Direct Marketing communications under Privacy and Electronic Communications Regulations (PECR).

The marketing must be directed to particular individuals. The ICO notes that in practice, "all relevant electronic messages (for example calls, faxes, texts and emails) are directed to someone, so they fall within this definition". This will also be the case for mail sent by post, where it is addressed to an individual.

The ICO and the courts have interpreted the definition of what activities are covered by Direct Marketing broadly.

Law and Guidance – Direct Marketing

DPA Section 11(3)

Direct Marketing is *...the communication (by whatever means)...of any advertising or marketing material...which is directed to particular individuals.*

ICO Direct Marketing Guidance

Version: 2.2 19th May 2016

This definition covers any advertising or marketing material, not just commercial marketing. All promotional material falls within this definition, including material promoting the aims of not-for-profit organisations....It will also cover any messages which include some marketing elements, even if that is not their main purpose. (Para. 35).

Direct marketing...also includes promoting an organisation's aims and ideals. This means that the direct marketing rules in the DPA and PECR will apply to the promotional, campaigning and fundraising activities of not-for-profit organisations. (Para. 44).

Not-for-profit organisations need to be aware that the definition of direct marketing will cover any messages that contain marketing elements even if this is not the main purpose of the message. (Para. 46).

DPA Section 11(1)

Right to prevent processing for purposes of direct marketing:

An individual is entitled at any time by notice in writing to a data controller to require the data controller...to cease, or not to begin, processing for the purposes of direct marketing personal data in respect of which he is the data subject.

This means that a significant number of purposes for which charities want to collect and use personal information, and so a significant amount of communication from charities, will fall within the definition of Direct Marketing.

These communications will need to comply with the requirements of both the DPA and the PECR. For example, the use of personal information for the following purposes is likely to be covered by

the Direct Marketing definition:

- Newsletters
- Individual giving appeals
- Emergency appeals
- Events and promotional activities
- Campaigning
- Seeking legacies
- Lotteries

A.4. Other uses of personal data that Direct Marketing may affect

Other ways that use of personal information may intersect with Direct Marketing include:

(i) Selling and sharing personal data

Code of Fundraising Practice Section 6.5

The Code of Fundraising Practice has already been updated to address this issue, at Section 6.5. ("Organisations MUST NOT share personal data for payment with any other organisation for that organisation's marketing or fundraising purposes").

ICO Monetary penalty notices Paragraph 21

The ICO penalty notices issued in December 2016 reinforced this rule, with the ICO confirming "Charities that wish to share/sell their marketing lists with other organisations must ensure that their donors were made aware of this when the personal details were collected and that specific consent to pass on the details were obtained."

(ii) Administrative communications

Note:
In most cases, communications with an exclusively administrative purpose are not classed as Direct Marketing. However, there are some important exceptions. *See **A.3. – A.7. Administration sections** below.*

(iii) Market research

Note:
Genuine market research is not classed as Direct Marketing if certain measures are taken. *See **A.7. Administration – of other purposes** below.*

(iv) Re-use of publicly available information

Note:
Many organisations, either themselves or through the use of third party data broker organisations, obtain and make use of information from the public domain. This information often forms the basis of other activities, such as wealth screening or data matching, data cleansing and teleappending/telematching.

*For further guidance on data matching and data appending see **A.6**.*

For further guidance on Wealth Screening see www.ico.org.uk/charity

A.5. Administration – Introduction

Personal information will need to be collected and used for administrative proposes. Charities will need to communicate with an individual for administrative purposes.

The ICO recognises this, noting the distinction between administrative communications and outright Direct Marketing:

ICO Direct Marketing Guide
Version: 2.2 19th May 2016

Administrative communication	Direct Marketing
A charity makes an administrative telephone call to an individual who has set up direct debit donations with a high street fundraiser as they wish to confirm the individual's bank details. If the call simply confirms the details then it will not be covered by the direct marketing rules. (Para. 46).	However if the charity uses this administrative call to suggest that the individual increases their donation or provides any other information promoting the charity's work then this will mean that the call ceases to be purely administrative and the direct marketing rules will apply. (Para. 46).

As noted in the ICO's example above, if an administrative communication seeks to promote the aims of the charity; is campaigning or seeks to fundraise then it will be classed as Direct Marketing, and therefore must comply with the requirements of the DPA and PECR.

A.6. Administration – processing transactions (for example, payments)

Charities may need to collect and use personal information to process transactions – for example, payment of donations (and any related GiftAid), fulfil promotional activities (for example, events) and fulfil purchases from their shops.

The provision of personal information by an individual in order to fulfil the transaction does not mean that the charity has consent to send subsequent Direct Marketing.

However, the collection and use of personal information to process transactions could be used as an opportunity to outline your **Direct Marketing options** to the individual. This could be achieved via the following methods:

1. At the point of collection (i.e. when the personal information required for the transaction is being collected): provide your agreed options / methods for collecting their unambiguous consent to also use their personal information for Direct Marketing.

i.e. You are seeking to use the personal information you need for the transaction for further purposes (i.e. Direct Marketing purpose(s))...

2. At the point of collection (i.e. when the personal information required for the transaction is being collected):

   provide a link to where the individual can then provide their personal information again, along with their unambiguous consent for Direct Marketing.

i.e. You are treating the individual as if they had come directly to where they can provide their personal information for Direct Marketing.

In both of these cases, you would use opt-in boxes, buttons, switches or slide-bars so you have a record* that an individual has given their unambiguous agreement to the use of their personal information for each different Direct Marketing purpose and each channel you wish to use.

***Note:**

What constitutes a record of consent is discussed in **B.6. The future – what GDPR means for consent and legitimate interests**

3. Use the acknowledgement / "thank you" sent to confirm the transaction to outline details of your Direct Marketing options.

   Example: Including a link on the acknowledgement / "thank you" to your Direct Marketing options.

   Example: Enclosing details of your Direct Marketing options, and a means for people to return these to you.

Note:

This communication can be justified **only once** – because you need to send the acknowledgement / "thank you" but do not have consent to send further unsolicited Direct Marketing without receiving their further consent.

Note:

Charities who sell products or service could rely on the "soft-opt in" as a basis for further Direct Marketing of these products or services via email. *See Section B – Lawfulness*.

A.7. Administration – of Direct Marketing

In order to maintain quality personal information for Direct Marketing purposes – i.e. to react to any change in relationships with donors; to administer their rights (for example, to object to Direct Marketing); to ensure consent remains valid – charities will need to send administrative communications to manage their Direct Marketing activity with individuals.

The ICO is clear that the act of sending an administrative communications about Direct Marketing requires the "processing" of personal information – and that this is therefore "*processing for the purposes of direct marketing personal data*". So this form of administration **is** covered by the definition of Direct Marketing.

This is important because it means that charities will need some form of consent in order to send administrative communications about Direct Marketing (as well as the actual Direct Marketing itself) via the channels that require consent (for example, email, text):

ICO Direct Marketing Guidance

Version: 2.2 19th May 2016

"Organisations cannot email or text an individual to ask for consent to future marketing messages. That email or text is in itself sent for the purposes of direct marketing, and so is subject to the same rules as other marketing texts and emails. And calls asking for consent are subject to the same rules as other marketing calls." (para 74).

Note:

For new donors, where the consent collected is clear, this does not pose a problem.

For existing donors – as part of the charity's self-assessment of their current circumstances (i.e. evaluating the standard of consent they currently operate to send Direct Marketing communications, and their overall degree of compliance) – the charity may conclude it wishes to contact individuals, i.e. where they currently hold their personal information but want to re-confirm and/or update the consent they hold.

- As noted above, Charities will need to assess the consent they currently hold in order to identify methods (channels) they believe they can use to make such administrative communications.
- *See **section B.7.** for more detail.*

A.8. Administration – Data Matching and Teleappending

Data Matching is the use of personal information you have been provided with by an individual for the purposes of trying to obtain (and then use) other personal information about the individual (which they have not chosen to provide to you themselves).

Teleappending is a form of data-matching, which focuses on the use of telephone numbers to obtain other personal information.

The ICO has noted that the use of personal information for the purposes of Data Matching and Teleappending should be regarded as separate purposes to Direct Marketing. The ICO will always uphold an individual's right to make specific decisions about the means by which they receive direct marketing. Therefore informed consent should be obtained in order to undertake Data Matching and Teleappending.

*See the ICO's **Direct Marketing guidance** for more detail.*

A.9. Administration – of other purposes

Charities will collect and use personal information for a number of other purposes not falling within the definition of Direct Marketing. For example:

1 **Complying with GiftAid requirements.**
HMRC rules govern what personal information is required to be collected and kept in order to meet GiftAid requirements.

2 **The management of staff.**
Staff and volunteers will need to provide certain information in order to be managed – including being paid; line management and other Human Resource issues.

3 **The management of volunteers.**
You will also need to provide certain information and updates to staff and volunteers – i.e. with essential information about their working environment or your expectations of them (such as updates to policies and procedures).

4 **The provision of services.**
Service users will need to provide certain information in order for you to provide efficient, safe, secure services.

5 **Market research**
The ICO Direct Marketing Guidance is clear:

ICO Direct Marketing Guidance

Version: 2.2 19th May 2016

"The direct marketing rules will not apply if an organisation contacts customers [or contracts a research firm to do so] to conduct genuine market research…as this will not involve the communication of advertising or marketing material.

"However, an organisation cannot avoid the direct marketing rules by labelling its message as a survey or market research if it is actually trying to sell goods or services, or to collect data to help it (or others) to contact people for marketing purposes at a later date. This is sometimes referred to as 'sugging' (selling under the guise of research). If the call or message includes any promotional material, or collects data to use in future marketing exercises, the call or message will be for direct marketing purposes. The organisation must say so, and comply with the DPA and PECR direct marketing rules.

"If an organisation claims it is simply conducting a survey when its real purpose (or one of its purposes) is to sell goods or services, generate leads, or collect data for marketing purposes, it will be breaching the DPA when it processes the data. It might also be in breach of PECR if it has called a number registered with the TPS, sent a text or email without consent, or instigated someone else to do so." (Para 38-40).

6 **Suppression**
You will need to maintain details of individual who have objected to Direct Marketing. This is often referred to as a suppression list.

The ICO is clear that you will need to maintain enough personal information to enable you to meet and adhere to individual's objections in the future:

ICO Direct Marketing Guidance

Version: 2.2 19th May 2016

"Organisations should maintain a 'suppression list' of people who have opted out or otherwise told that organisation directly that they do not want to receive marketing.

Note that individuals may ask an organisation to remove or delete their details from a database or marketing list. However, in most cases organisations should instead follow the marketing industry practice of suppressing their details.

Rather than deleting an individual's details entirely, suppression involves retaining just enough information to ensure that their preferences are respected in the future" (Para 190-192).

Note:

In all cases, there should be no automatic assumption that the staff member, volunteers or service users wants to receive Direct Marketing.

Their agreement should be sought as if they were any other individual.

Note:

Where individuals provide their personal information for non-Direct Marketing purposes, grounds other than consent may well justify the collection and use of the personal information. Remember however that preparatory work for Direct Marketing can count as a Direct Marketing purpose in itself.

Section summary

A. Purpose

Recommended actions to take:

1. Define the purposes for which your charity collects and uses personal information.
2. Confirm which purposes are Direct Marketing, and which are not.
3. For each Direct Marketing purpose, confirm what activities this includes and how any individuals are contacted, and document your rationale and legal basis for this in each case.
4. Publish your decisions in your Privacy Policy.

B: Establishing Lawfulness

This section will explain:

- What the Data Protection Act and Privacy Regulations require you to do when collecting and using personal data.
- How the requirements differ across different communication channels.
- How to obtain consent from an individual to collect and use their data, the risks and benefits of different methods and how long consent should be understood to last.
- When a "legitimate interests" condition may justify the processing of personal data.
- The General Data Protection Regulation (GDPR) and how this will affect the rules on consent and legitimate interests from May 2018.
- Some good practice recommendations and issues to address to ensure your practices are lawful.

B.1. Introduction to the Data Protection Act and Privacy Regulations

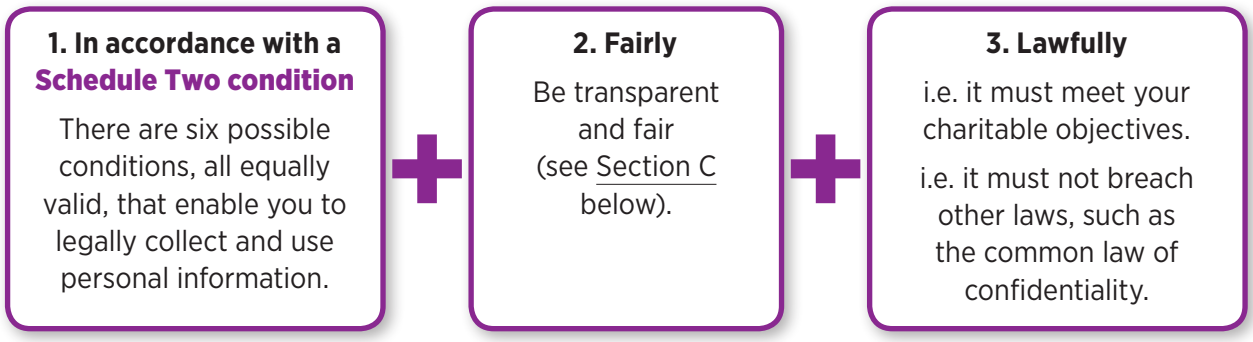
Having defined the purpose or purposes for which your charity wants to collect and use personal information, the next stage is to determine how this processing of personal information will be lawful.

This section focuses on lawfulness in relation to Direct Marketing because this requires the collection and use (the processing) of personal data.

Two laws currently define how the collection and use of personal information for Direct Marketing purposes must be managed: the **Data Protection 1998 (DPA)** and the **Privacy and Electronic Communication Regulations 2003 (PECR)**.

DPA

The First Principle of the DPA requires that (non-sensitive) personal information is processed



PECR

In 2003 the PECR added further rules, as well as having to comply with the DPA, when using personal information for electronic methods of Direct Marketing.

Different rules therefore apply, depending on which communication channel (or channels) you use for Direct Marketing.

The next two pages summarise the current requirements for each channel.

Then follows detail on the key terms of consent and legitimate interests – looking at both the current laws and the General Data Protection Regulation (GDPR), due to become law on 25th May 2018.

B.2. Summary of channels – email, SMS, automated calls, fax, live calls and post

<table>
<tr><th></th><th>Email / SMS / Automated calls / Fax</th><th>Live Calls</th><th>Post</th></tr>
<tr><td rowspan="3">PECR</td><td>Always requires consent.</td><td>Consent not only legal basis for contact.</td><td>Not covered by PECR – as not electronic.</td></tr>
<tr><td>Consent means doing something positive (for example, ticking a box), not relying on using pre-ticked boxes or on someone not opting out.</td><td rowspan="2">Must consider whether the person has
(i) previously objected to you contacting them (i.e. said no to you), i.e. “opted-out” and on your suppression list
(ii) already registered with Telephone Preference Service (TPS) – i.e. already indicated their objection to being called.</td><td rowspan="2">You only have to comply with the requirements of the DPA to justify your collection and use of personal information to send post.</td></tr>
<tr><td>“consent for electronic marketing messages is more tightly defined than in other contexts, and must be extremely clear and specific.” (Direct Marketing Guidance Version: 2.2; 19th May 2016, para. 63)</td></tr>
<tr><td rowspan="2">DPA</td><td rowspan="2">Consent must have already been obtained in order to comply with the requirements of the PECR.</td><td>Specific consent (ie. consent to be contacted by you at this number) needed for people registered on TPS or who have previously objected to you. Consent or possible use of Legitimate Interests for people not registered on TPS / who have not previously objected to you.</td><td>Consent or possible use of Legitimate Interests.</td></tr>
<tr><td colspan="2">Consent may not be needed to undertake direct marketing by post or phone call (unless the individual is registered with the Telephone Preference Service) if another processing condition can be relied on, but the ICO considers gaining consent to do this to be good practice and the most advisable approach.” (Privacy Notices, Transparency and Control Code of Practice; Version 1.0.27; 07 Oct 2016; Page 9).</td></tr>
</table>

Notes

PECR Soft opt-in

For existing customers, organisations can send commercial marketing texts or emails if:

The details were obtained during the sale (or negotiations for a sale) of a product or service to the individual

+ the organisation will only then market their own similar products or services

+ the organisation gives the individual a simple opportunity to refuse or opt out of the marketing – at the point of collecting the information and in every subsequent message.

However, it does **not** apply to non-commercial promotions (eg. charity fundraising or political campaigning). Nor does it apply to prospective customers or new contacts (eg. from bought in lists).

Direct Marketing Guidance

Version: 2.2 19th May 2016

"Not-for-profit organisations might be able to use the soft opt-in for any commercial products or services they offer...[they] will not be able to rely on the soft opt-in when sending campaigning texts or emails, even to existing supporters. In other words, texts or emails promoting the aims or ideals of an organisation can only be sent with specific consent." (Para 50, 131-138).

Organisations can rely on the DPA "legitimate interests" condition to justify the collection and use of personal information to (i) make calls to people not on TPS and not on your suppression lists, and (ii) to send post.

i.e. you believe you have legitimate interests, and these interests are not causing any undue harm to the rights and freedoms or legitimate interests of the individual.

In such cases, you are not therefore seeking or relying on an individual's consent; instead you are relying on "legitimate interests" and will react if an individual objects or "opts out" (ie you will cease direct marketing activity in accordance with their chosen preferences and update your suppression list accordingly).

N.B: You should read **B.5. Legitimate interests** below for key questions you must be able to answer before acting on this condition.

It is worth noting the direction in which regulation is travelling: the e-Privacy Directive (from where our PECR comes from) is being reviewed in light of the GDPR.

The e-Privacy Directive (from where our PECR comes from) is being reviewed in light of the GDPR and is now expected to be introduced as regulation on the same date (25th May 2018). Part of the review questions the current approach with regards to live calls. The ICO responded as follows:

"There should be a harmonised opt-in approach with a clear set of rules...These should be consistent with provisions in the GDPR. In our view, the privacy implications of receiving unwanted telemarketing calls are at least as great - and arguably greater, particularly for some vulnerable people - than other channels which already require an opt-in (eg electronic mail)."

ICO response to question 8 of the Questionnaire For The Public Consultation On The Evaluation And Review Of The E-Privacy Directive, 1st July 2016.

The current draft ePrivacy Regulation sets a default position of opt-in to all electronic marketing, including live calls, although member states can choose to legislate for an opt-out system for live calls that don't involve automatic dialling.

B.3. Consent – issues to consider when relying on consent

If a channel you wish to use to send Direct Marketing requires the consent of the individual, consider the following law and guidance on obtaining that consent:

DPA Schedule 2, Condition 1

The data subject has given his consent to the processing.

Notes:

The DPA does not contain a definition of consent. This meant organisations often took "consent" as being sufficient if it was "implied" – for example, someone had not "opted out."

Using an opt-out also helped organisations provide for an individual's right to object to Direct Marketing – i.e. someone could object (opt-out) if they did not wish the organisation to rely on their "implied consent."

There are no legal definitions for "opt-in" and "opt-out;" they are marketing terms used to address the key issue of consent.

Directive Art. 2(h)

Although the DPA did not contain a definition for consent, the EU Directive did have a definition. This is significant, because our DPA implements the Directive in the UK.

The Directive definition of consent is that consent should be a

"freely given, specific [both specific to the channel of communication and specific to the charity] and informed indication of [an individual's] wishes by which the data subject signifies [their] agreement to personal data relating to [them] being processed."

This definition was therefore always the standard of consent that organisation should have been seeking.

Direct Marketing Guidance

Version: 2.2 19th May 2016

The ICO recognised this in their Direct Marketing Guidance:

"...it is good practice to have explicit consent...Even implied consent must still be freely given, specific and informed, and must still involve a positive action indicating agreement" (para. 64 and 65).

ICO Penalty notices December 2016 Paragraphs 7 and 21

The ICO has recently reconfirmed that

"...the DPA implements European legislation (Directive 95 / 46 / EC) aimed at the protection of the individual's fundamental right to the protection of personal data. The DPA must be applied so as to give effect to that Directive."

"consent must be freely given, specific and informed, and involve a positive indication signifying the data subject's agreement."

Privacy Notices, Transparency and Control Code of Practice

Version 1.0.27 07 Oct 2016 Page 8-9

"When relying on consent, your method of obtaining it should:

- *be displayed clearly and prominently;*
- *ask individuals to positively opt-in, in line with good practice; and*
- *give them sufficient information to make a choice. If your consent mechanism consists solely of an "I agree" box with no supporting information, then users are unlikely to be fully informed and the consent cannot be considered valid.*

If you want individuals to consent to direct marketing, you should have a separate unticked opt-in box for this, prominently displayed."

(i) Coercion, unduly incentivising or making consent to marketing a condition of subscribing to / applying for a service or activity:

Direct Marketing Guidance

Version: 2.2 19th May 2016

The ICO also recommends that organisations

"do not make consent to marketing a condition of subscribing to a service unless they can clearly demonstrate how consent to marketing is necessary for the service and why consent cannot be sought separately." (para 66).

"should not coerce or unduly incentivise people to consent, or penalise anyone who refuses."

The ICO cite a case involving the Universities and Colleges Admissions Service (UCAS): their application form used opt-out for marketing from commercial companies. The wording of the opt-out also meant that unticking the boxes would result in the applicant not receiving information about career opportunities and education providers or health information.

The ICO ruled that this approach meant applicants felt obliged to let UCAS use their information for commercial purposes otherwise they would potentially miss out on important information about their career or education. (para 60).

(ii) The difference between seeking consent and ensuring people are informed:

Privacy Notices, Transparency and Control Code of Practice

Version 1.0.27 07 Oct 2016 Page 8

The ICO notes the important distinction between seeking consent and ensuring people are informed about your intentions:

"There is a fundamental difference between telling a person how you're going to use their personal information and getting their consent."

ICO Penalty notices December 2016 paragraph 21

This was reflected in the ICO Penalty notices issued in December 2016:

"Informing individuals that their details will be [used for a certain purpose] is neither freely given nor specific and does not amount to a positive indication of consent"

B.4. Consent – ways for individuals to express consent

The two key means of enabling individuals to express consent for Direct Marketing communications are by "opting-in" (or signifying that they wish to receive marketing messages) or by "opting-out" (or signifying that they object to receiving marketing messages). Currently, either of these methods may achieve lawful consent if they involve "some form of communication or positive action by which the individual clearly and knowingly indicates their agreement" (ICO Direct Marketing Guidance, 2016). However, there are some particular risks in relying on opt-out alone as evidence of consent.

This section gives some charity-based examples of "opt-in" and opt-out" in practice and discusses where the merits and risks lie.

(i) Example of "opt-in" consent good practice

I am happy for my data to be used to:

Contact me about ways to provide financial support ☐

Contact me about opportunities to volunteer / get involved in fundraising ☐

Contact me about opportunities to sign petitions ☐

Share my data with charity X which may have information of interest to me ☐

I am happy to be contacted via:

post ☐

email ☐

telephone ☐

text message ☐

recorded call ☐

Note that this example:

- Includes a clear separation of each marketing channel – the consent requested is specific in that it does not ask the individual to tick one box to approve multiple channels. This means there is no room for misinterpretation, either by the individual in knowing what they have consented to, or from the charity in terms of evidencing this consent.
- Includes a clear separation of each purpose and is specific in what the communication purpose is (for example, to "contact me about ways to provide financial support"). It does not ask the individual to tick one box to approve multiple communications with different purposes (for example, "financial support and volunteering opportunities"). Once you have assessed your purpose and how alike or different your purposes are to each other *(see **Section A: Purpose** for more detail)*, you need to consider if it is necessary to separate your purposes into multiple consent questions, as the example above has done.

The organisation should consider providing a marketing communication channel for each separate, specific purpose where it is technically possible and considered desirable by the organisation, to further tailor the individual's choice on which purposes they wish their personal information to be use for, and via which channels.

(ii) Examples of "opt-out" consent and potential risks of using this approach

Registration form

By submitting this registration form, you indicate your consent to receiving email marketing messages from us. If you do not want to receive such messages, tick here: ☐

Note that this approach must:

- require the user to take a positive action to signal their consent (in these cases, submitting the registration form and providing their phone number).
- include a suitably prominent means of opting-out for those who do not wish to receive marketing messages.
- ensure that the individual's wish to consent to one action (in these examples, registration and making a donation) should not require or be dependent on their consent to receive marketing messages – see the guidance above on coercion, unduly incentivise and make consent to marketing a condition of subscribing to / applying for a service or activity.
- be prominently displayed. It cannot be buried in the small print or leave the individual with any justifiable cause to argue that they could not have reasonably known

Despite these steps, there remains the risk that an approach which relies on opt-out consent may not be considered an "**unambiguous** (i.e. not open to more than one interpretation) indication" of the persons wishes by a "clear **affirmative** action." This is because an individual may claim they only wished to submit their registration form / make a donation – and did not see, recognise the impact of, or misunderstood, any statement relating to the use of their personal information for Direct Marketing.

The following example, in which a charity attempts to secure opt-out consent by the individual entering their telephone number illustrates where opt-out consent may be ambiguous, and affirmative action taken by the individual may be unclear:

Donation form			
First Name		Surname	
Address			
Postcode		Phone*	
*As part of [charity name] we'd love to call you, to tell you about the amazing difference you have made and how you can donate and support our work. Please only give us your number if you're happy for us to contact you in this way.			

In this example:

- If the individual wishes to give their phone number for administrative contact, but does not wish to receive direct marketing, there is no option for them to do so. If they do wish to give

their phone number, but for administrative contact only, this is dependent on them signing up for direct marketing.

- An individual could also reasonably misinterpret the asterisk next to the "phone" option as required information as this is a standard symbol used by many organisations to indicate essential data for processing the request.

A charity using opt-out methods would need to explain, if questioned by the donor or ICO, or when considering the wider public perception, why clearer methods that could have been used to obtain unambiguous consent were consciously not used.

iii) Opt-out consent and GDPR

A charity using such methods must also consider that this consent risks falling short of the standards set out in GDPR and would therefore lapse in May 2018. This includes the standards that consent should be "clearly distinguishable from the other matters" (Art 7(2)) and that it should be a clear, affirmative action ("silence, pre-ticked boxes or inactivity should not constitute consent" (Rec 32)).

There is a further risk that the GDPR requirement to *"demonstrate that the data subject has consented to processing of [their] personal data"* is not met – because the evidence is open to more than one interpretation ***(See section B7 below for more information on what GDPR will mean for Consent).***

These concerns must be balanced against any perceived benefit of using such methods.

B.5. Consent – defining how long consent lasts

Fundraising organisations should refresh their consent with individuals within a reasonable timescale of them agreeing to communications. The DPA does not define what "reasonable" means in terms of defining how long consent can be taken to last. Consent under PECR is expressly considered to be 'for the time being'. However, the NCVO's working group on consent in September 2016 proposed that large fundraising organisations that undertake mass fundraising campaigns should consider refreshing consent at least every 24 months. There may be specific circumstances where a prescribed 24 month limit is not appropriate but these should be justified and necessary. See below for some factors that may affect how frequently consent is refreshed.

The core question that organisations should consider in establishing their timescale for refreshing consent is not what the organisation would consider "reasonable" for its own purposes, but: for how long would the individual consider it reasonable to be contacted before they were asked to renew consent?

Direct Marketing Guidance
Version: 2.2 19th May 2016

There is no fixed time limit after which consent automatically expires. However, consent will not remain valid forever. How long consent remains valid will depend on the context – the question is whether it is still reasonable to treat it as an ongoing indication of the person's current wishes. (Para 97).

Consent lasts as long as circumstances remain the same, and will expire if there is a significant change in circumstances. (Para 63).

Even if consent is not explicitly withdrawn, it will become harder to rely on as a genuine indication of the person's wishes as time passes.

Consent under PECR is expressly considered to be 'for the time being'. We consider this implies a period of continuity and stability, and that any significant change in circumstances is likely to mean that consent comes to an end. (para 99).

In the case of new donors, this question may be easier to resolve if you set expectations with the individual from the start and let them know in your communications of your intention to refresh consent with them at a pre-defined date in the future.

Other factors charities may wish to consider in determining how urgent a priority it may be to refresh consent with individual donors may include (but are not limited to):

How big is your organisation / campaign?

The NCVO's working group on consent in September 2016 proposed that large fundraising organisations that undertake mass fundraising campaigns should refresh consent at least every 24 months. For smaller organisations, the individual may not expect a consent refresh as frequently.

How often are you contacting the individual?

If contact is weekly or monthly, it may be necessary to set a shorter timescale for refresh than if you only contact them once a year.

How intrusive is the channel of communication you are using?

Some forms of communication may be regarded by the individual as more intrusive than others. For example, although the law does not reflect this in terms of requiring consent, be mindful that if you are calling somebody on the telephone, the individual may view this as a more intrusive fundraising approach than sending them an email communication and the recipient may consequently consider it reasonable for a shorter timescale to elapse before refreshing consent.

Is the cause or project time-limited? / Is the organisation's fundraising limited to emergency appeals?

For example, if the donor has agreed to receive communications regarding a specific, time-limited project it may be reasonable to assume that they would like to receive communications for the lifetime of that specific project before renewal, while greater frequency may be required if the cause is more open-ended. Likewise, if you only do appeals around natural disasters it may be sensible to refresh consent following an appeal rather than setting a regular timeframe.

What is the nature of the relationship with the donor or potential donor?

For example, if there is regular and positive communication from the donor in response to your communications, it may be reasonable to refresh consent less frequently than if you are sending communications regularly with no response. (This does not mean that a 'long standing relationship' could in and of itself be argued to constitute consent).

The value of defining a "reasonable" time period

The examples below shows the value of the fundraising organisation establishing clear timescales for how long the donor's consent is taken to last before it needs to be refreshed.

Example 1: Charity X have a number of personal emails from individuals on their fundraising database.

- They have continued to send communications to these individuals, but have not had any communications from them in response in years.
- They have no clear policy on how long they expect consent should last and after several years on the database, the charity are unsure whether the consents they had in place for these individuals continue to be active.
- As a result, they cannot be sure that they still have permission to email these donors with their Direct Marketing, or to seek refreshed consent. They are forced to delete the email addresses from their database or risk breaking the law by contacting the individuals concerned to update their permissions.

Example 2: Charity Y have analysed their communications with supporters and developed a policy that when they get consent from a donor to contact them, they will operate on the understanding that this permission lasts 2 years.

- When they first receive the donor's consent to send them fundraising emails, the charity make the donor aware that they will assume their consent lasts for two years in accordance with this policy (unless the donor opts out before this point).
- They contact the donor before the 2 year period has elapsed to check that they are still happy to receive these communications, safe in the knowledge that permission to approach the donor to refresh their consent is still active.
- They may also outline other new Direct Marketing purposes that the individual may previously have been unaware of (for example, because the charity has developed new fundraising activities), and seek their consent for these.
- Where a donor does not respond to the refresh request, they delete them from their database at the end of the 2 year period, letting the individual know that they have done so and why.

B.6. Legitimate interests

The Data Protection Act recognises that an organisation may have legitimate reasons for processing personal data that the other conditions for processing do not specifically deal with. In a limited number of circumstances therefore, a charity may be able to justify communicating with an individual on the basis of the charity's legitimate interests.

The legitimate interests condition cannot be assumed to apply simply because a charity has an interest in contacting the individual. For a Direct Marketing approach to have the possibility of relying on your legitimate interests, it must strike the balance between your legitimate interests and

the privacy expectations of the individual:

DPA Schedule 2, Condition 6

The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.*

***Note:**

Your organisation is the Data Controller – i.e. it is the organisation who decides the purposes for which personal information will be collected and used, and the manner in which it is processed.

Any proposed reliance on Legitimate Interests should therefore consider

- the reasonable expectations of individuals, based on their current or proposed relationship with you
- why an individual would reasonably expect the use of their personal information in this way without their consent
- why the rights and freedoms of the individuals are not going to be unduly harmed, including
  - the measures you will have in place to manage objections;
  - the nature of Direct Marketing you will be sending them, and
  - the number of times Direct Marketing communication will be sent on the basis of legitimate interests.

B.7. The future – what GDPR means for consent and legitimate interests

The GDPR will strengthen provisions around consent and legitimate interests.

Consent – GDPR

GDPR Art. 4(11)

"...any freely given, specific, informed and unambiguous indication of [an individual's] wishes...[either] by a statement or by a clear affirmative action signifies agreement to the processing of [their] personal data

GDPR

The GDPR outlines further detail on how consent should be interpreted:

Methods to collect consent (Recital 32)

"such as by a written statement, including by electronic means, or an oral statement."

"This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data."

"Silence, pre-ticked boxes or inactivity should not therefore constitute consent."

Proof of consent (Art. 7(1))

Organisations have to be able to "demonstrate that the data subject has consented to processing of [their] personal data."

Note:

Charities will need to retain sufficient information about when a consent was obtained, and for what Direct Marketing purpose(s) consent was provided for.

- Electronically, this could mean the system logging details of when the consent was provide.
- Verbal consent could be recorded by retaining a note of when the verbal consent was obtained and what fair processing / privacy information was provided – for example, a note confirming that "Privacy Notice #1 was discussed" and the date. Confirmation could subsequently be provided to the individual.

Consent as part of a wider written declaration by the individual (Art 7(2))

"The request for consent shall be presented in a manner which is clearly distinguishable from the other matters".

Changes in consent (Art. 7(3))

Individuals *"shall have the right to withdraw [their] consent at any time."*

[This] shall not affect the lawfulness of processing based on consent before its withdrawal.

It shall be as easy to withdraw as to give consent.

Consent linked to purposes (Recitals 32 and 43)

As already mentioned in ***Section A – Purposes*** above, consent is linked to purpose:

"Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case..."

"Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them."

Privacy Notices, Transparency and Control Code of Practice

Version 1.0.27 07 Oct 2016 Page 9

"if you are processing information for a range of purposes you should:

- *explain the different ways you will use their information; and*
- *provide a clear and simple way for them to indicate they agree to different types of processing. In other words, people should not be forced to agree to several types of processing simply because your privacy notice only includes an option to agree or disagree to all. People may wish to consent to their information being used for one purpose but not another."*

Legitimate interests – GDPR

GDPR Art. 6(1)(f)

...necessary for the purposes of [your] legitimate interests...except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject...

GDPR Recitals:

The GDPR outlines further detail on how legitimate interests should be interpreted:

(Recital 47)

The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(Recital 47)

When assessing your legitimate interests, consider *"...the reasonable expectations of [individuals] based on their relationship with [your organisation]."*

Legitimate interest could exist, for example, where *"there is a relevant and appropriate relationship between the [individual] and [your organisation] in situations such as where the [individual] is a client or in the service of [your organisation]."*

Always consider *"whether [an individual] can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place."*

"The interests and fundamental rights of the [individual] could in particular override the interest of [your organisation] where personal data are processed in circumstances where [individuals] do not reasonably expect further processing."

B.8. Recommendations and issues to be addressed

Charities must have a clear understanding of the basis on which they will justify their collection and use of personal information for their Direct Marketing purposes.

Recommendation 1

Obtain GDPR-standard consent using opt-in boxes, buttons, switches, slide-bars, user preference management tools or other such means that result in your organisation having a record that an individual has given their unambiguous agreement to the use of their personal information for

- each different Direct Marketing purpose you wish to collect and use personal information for, and
- each channel you wish to use

Additionally, communications should include a mechanism to withdraw consent easily at any time.

Rationale:

The references made in this Section to the Directive and GDPR definitions of consent, the ICO's Codes of Practice and Guidance, and the desire of the Fundraising Regulator to ensure that the sector adheres to good practice, all point to opt-in methods as the clearest, safest, most future-proof way of collecting and demonstrating consent.

This is because they require a positive choice by the individual to give clear, unambiguous consent for specific Direct Marketing purposes.

Review of compliance

As noted in Section A.7. Administration – of Direct Marketing, charities may, for existing donors, want to self-assess their current circumstances (i.e. evaluating the standard of consent they currently operate to send Direct Marketing communications, and their overall degree of compliance).

- Charities may conclude they wish to contact individuals, i.e. where they currently hold their personal information but want to re-confirm and/or update the standard of consent they hold.
- To make such contact, charities will need to first assess the standard of consent they currently hold in order to identify methods (channels) they believe they can use to make such administrative communications (because the act of making an administrative communications about Direct Marketing requires the "processing" of personal information – and that this is therefore *"processing for the purposes of direct marketing personal data"*).
- See the separate Consent self-assessment tool at www.fundraisingregulator.org.uk as a starting point for making an assessment.

Recommendation 2

Only rely on legitimate interests to justify using post to send Direct Marketing where you have published the "balancing exercise" you have undertaken to justify using legitimate interests rather than unambiguous consent.

To note: It would not be possible for charities which have already committed to opt-in communication models to rely on this condition as this would not be opt-in.

Rationale:

Individuals may have received Direct Marketing via post for many years, without complaint or objection. A charity wishing to continue using this channel for Direct Marketing should be able to outline what their legitimate interests are, why the posting of Direct Marketing is necessary for the purpose of pursuing that legitimate interest, and why this would not harm the rights and freedoms or legitimate interests of the individual(s) to such an extent that it is unwarranted.

Recommendation 3

Do not rely on legitimate interests unless it can be shown that the data was obtained fairly and lawfully. The provenance of data and the specificity of consent to process data should be considered.

Rationale:

Consent to share data with "Charities" or "selected third parties" is not specific enough for data sharing to be fair and lawful. Legitimate interest cannot be used if the data was not obtained fairly and lawfully.

Recommendation 4

Do not rely on legitimate interests to make live calls to non-TPS and non-previous object numbers.

Rationale:

The privacy implications of live calls are arguably as great or greater than other channels that already require consent. Given the number of people registered with the TPS – and the ICO's feedback to the consultation on the Privacy Regulations (as referenced above) it is likely that all live calls will be based on consent in the future.

Recommendation 5

Define your approach to refreshing consent with individuals within a reasonable timescale of them agreeing to communications.

Section summary

B. Lawfulness

Recommended actions to take:

For each Direct Marketing purpose,

1. Define which channel or channels you wish to use to communicate with individuals.
2. Where you will rely on consent,
    a. outline how you will seek "unambiguous" consent via individuals giving "a statement" or "a clear affirmative action" and
    b. define how long consent will last in each case.
3. Where you seek to rely on legitimate interests, define and publish the outcome of your balancing exercise.

C: Establishing Fairness and Transparency

This section will help you understand:

- What the law requires and what guidance recommends you do to ensure you are fair and transparent with the individual regarding their data.
- The privacy information you must provide to comply with the GDPR fairness and transparency requirements.
- The rights of individuals to access the personal information you collect and hold on them and their right to object to Direct Marketing.
- How the GDPR and the Fundraising Preference Service will strengthen the individual's right to object.

Having defined what Direct Marketing activities your charity wants to use personal information for (**Section A: Purposes**) and the basis on which you plan to obtain and use personal data – especially which channels of communication you wish to use (**Section B: Lawfulness**) the next step is to define how your charity will ensure individuals are

i. treated fairly;

ii. know about your proposed use (or uses) of their personal information, and

iii. can use their rights to manage their personal information

C.1. The law on fairness and transparency

DPA Principle 1

"Personal data shall be processed fairly..."

DPA Part II, Schedule 1, 2(3)

Fair Processing / Privacy Notices – to be provided to the individual at the point their personal information is collected

The DPA says that in order for the processing to be fair, you have to make certain information available to the individuals who are providing their personal information to you.

This information is

"(a) the identity of the data controller [i.e. your charity name],

(c) the purpose or purposes for which the data are intended to be processed, and

(d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair."

GDPR Art. 5(1)(a)

"Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')."

GDPR Art. 7(2)

If you seek consent as part of another process which also concerns other matters (for example, an application form, or online transaction),

"the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language."

Privacy Notices, Transparency and Control Code of Practice

Version 1.0.27 07 Oct 2016 Page 33

The GDPR includes rules on giving privacy information to individuals. The ICO notes that

"These are more detailed and specific than in the DPA and place an emphasis on making privacy notices understandable and accessible. Data controllers are expected to take 'appropriate measures'.

"Data controllers may need to include more information in their privacy notices, but we believe that if you follow the good practice recommendations in this code you will be well placed to comply with the GDPR regime.

"There is still discretion for data controllers to consider where the information required by GDPR should be displayed in different layers of a notice."

C.2. Table of the privacy information you must provide to comply with the GDPR fairness and transparency requirements

from the ICO's *Privacy Notices, Transparency and Control Code of Practice*, pages 33-35

GDPR Art. 13

Information to be provided where personal data **are collected** from the data subject

What information must be supplied?	Data collected directly from data subject	Data not collected directly from data subject
Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the **legal basis** for the processing	✓	✓
The **legitimate interests** of the controller or third party, where applicable	✓	✓
Categories of personal data		✓

GDPR Art. 14
Information to be provided where personal data **have not been obtained** from the data subject

What information must be supplied?	Data collected directly from data subject	Data not collected directly from data subject
Any recipient or categories of recipients of the personal data.	✓	✓
Details of transfers to third country and safeguards.	✓	✓
Retention period or criteria used to determine the retention period.	✓	✓
The existence of each of data subject's rights.	✓	✓
The **right to withdraw consent** at any time, where relevant.	✓	✓
The **right to lodge a complaint** with a supervisory authority.	✓	✓
The **source the personal data originates from** and whether it came from publicly accessible sources.		✓
Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.	✓	
The **existence** of automated decision making, including **profiling** and information about how decisions are made, the significance and the consequences.	✓	✓

When should information be provided?	
Data collected directly from data subject	**Data not collected directly from data subject**
At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month); If the data are used to communicate with the individual, at the latest, when the first communication takes place; or If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

ICO Penalty notices December 2016

The ICO highlighted the lack of sufficient transparency in the Penalty Notices they issued against 2 charities in December 2016. A lack of openness and transparent was found to have denied individuals the ability to use their legal rights to object and, more broadly, control what happens to their personal information:

"Supporters have not been provided with sufficient information to enable them to understand what would be done with their personal data [in this case, in relation to wealth screening] and thereby to enable them to make informed decisions on whether or not they wished to object."

"...by failing adequately to explain to data subjects how their personal data would be used, the [charities have] deprived them of control and informed decision-making about their personal data to a significant extent."

Examples of fair processing notices considered insufficient were as follows:

"From time to time, we may allow other similar or partner organisations to contact our supporters. If you do not wish to hear from them, tick here" ; and

"[We] may allow other organisations whose aims are in sympathy with our own or whose offers will benefit animal welfare to contact our supporters. If you do not wish to hear from them please tick here"

Both were found to be "unduly vague and / or ambiguous" about the planned data sharing, and did not make reference to the planned wealth screening or data/tele-matching.

The ICO's enforcement priorities reflect the key messages from its 2016 ***Privacy Notices, Transparency and Control Code of Practice***. This Code also includes reference to the GDPR.

C.3. Summary of the key messages from the ICO's *Privacy Notices, Transparency and Control Code of Practice*

1 About the code

"It is often argued that people's expectations about personal data are changing. People are increasingly willing to share information on social media and to allow their data to be collected by mobile apps, and they are also unwilling to read lengthy privacy notices.

These factors are sometimes used to support the view that they are relatively unconcerned that their data is being collected and processed. However, there is also evidence that people do have concerns about how organisations handle their data and want to retain some control over its further use.

Therefore, it is still of paramount importance for organisations to be transparent about their processing and comply with the legal requirements to provide privacy information.

Moreover, many organisations embrace transparency as a means of building trust and confidence with their consumers and use it as a means of distinguishing themselves from their competitors."

Give individuals appropriate control and choice

"Where you need consent from an individual in order to process their information you need to explain what you are asking them to agree to and why. This will often go hand in hand with providing privacy notices.

You should always be honest with the public and not lead them to believe that they can exercise choice over the collection and use of their personal information when in reality they cannot.

There are some cases in which consent is not relevant, for example if individuals are required by law to provide their personal details. Giving people control and choice over how their personal data will be processed will not always be applicable in other situations, for example in an employer/employee relationship."

2 Why should you provide effective privacy information?

"Following good practice in providing privacy notices helps you to deal with people in a clear and transparent way and empower them. This makes good sense for any organisation and is key to developing trust with customers or citizens."

3 What should you include in your privacy notice?

You should tell people more than just the basic information "where you think that not telling people will make your processing of that information unfair. This could be the case if an individual is unlikely to know that you use their information for a particular purpose..."

4 Where should you deliver privacy information to individuals?

"You should not necessarily restrict your privacy notice to a single document or page on your website. The term 'privacy notice' is often used as a shorthand term, but rather than seeing the task as delivering a single notice it is better to think of it as providing privacy information in a range of ways. All of the information you are giving people about how you are processing their data, taken together, constitutes the privacy information."

This section also addresses:

- Emergency situations
- The Layered approach
- Using just-in-time notices
- Using icons and symbols
- Adapting to mobile devices and smaller screens

5 When should you actively communicate privacy information?

"...try to put yourself in the position of the people you're collecting information about. You need to understand the level of knowledge your intended audience has about how their data is collected and what is done with it. This will help you decide when to give them privacy information.

If an individual would not reasonably expect what you will do with their information you need to actively provide privacy information, rather than simply making it available for them to look for themselves, for example on your website.

If it is reasonable for someone to expect that you will use their information for an intended purpose, you are less likely to need to actively explain it to them and can instead make privacy information available if they look for it."

6 How should you write a privacy notice?

You should:

- use clear, straightforward language;
- adopt a simple style that your audience will find easy to understand;
- not assume that everybody has the same level of understanding as you;
- avoid confusing terminology or legalistic language;
- align to your house style. Using expertise, for example in-house copywriters can help it fit with the style and approach your customers expect;
- align with your organisation's values and principles. Doing so means that people will be more inclined to read privacy notices, understand them and trust your handling of their information;
- be truthful. Don't offer people choices that are counter-intuitive or misleading;

This section also addresses:

- Privacy notices for a wide range of individuals
- Privacy notices for vulnerable individuals
- Privacy notices for people whose first language is not English

7 Your privacy notice checklist

See the appendix to this document for the ICO's checklist

8 Privacy notices in practice

This section addresses:

- Sharing information
- Selling information
- Big data

Individual rights

Individuals have two key rights in relation to Direct Marketing:

1. A right of access to the personal information you collect and hold on them.
    - This right can be accessed by an individual who makes a "subject access request" to a charity.
    - Charities should therefore consider how to process such requests – i.e. to verify the identity of the requester and consider whether any exemptions apply to restrict access*
    - Charities should also consider how the data they hold would be viewed by the individual should they request access to it – for example, how any emails, records of assessment or notes about a data subject may be viewed by the individual concerned.
2. A right to object to Direct Marketing
    - This is the right to object to receiving Direct Marketing.
    - This is where we get the term "opt-out" from – because people have a right to object to (opt-out of) receiving Direct Marketing.

- Formally this is known as a Section 11 notice, because such requests for Direct Marketing to be stopped are made by individuals under section 11 of the DPA.

Charities should therefore include details of these rights in their Privacy Policies.

* This is not intended to be a full guide to Subject Access. The ICO's Subject Access Code of Practice can be accessed here.

DPA Section7
Right of access to personal data

"an individual is entitled…to have communicated to him in an intelligible form…the information constituting any personal data of which that individual is the data subject"

DPA Section 11
Right to prevent processing for purposes of direct marketing

"An individual is entitled at any time by notice in writing to a data controller, to require the data controller to cease, or not to begin, processing for the purposes of direct marketing personal data in respect of which [they are] the data subject."

Fundraising Preference Service (FPS)

- Individuals will specify to the Fundraising Regulator the charities they no longer want to hear from
- The Fundraising Regulator will ensure charities are then notified of these suppressions (i.e. those people opting out) and that they comply, through a largely automated process
- The opt-out will cover all charities and all forms of communication with a named individual (email, text, telephone and addressed mail) – rather than just larger charities and their "fundraising communications."
- The FPS opt-out will have the statutory force of a Data Protection Act Section 11 Notice to cease direct marketing.

GDPR Article 21
The GDPR develops the rights to object to direct marketing.

Article 21 states that individuals still have the right to object, but adds an obligation on organisations to "explicitly" bring this right to the attention of the individual, regardless of the communication channel you are using.

This must be communicated "clearly and separately from any other information" and "at the latest at the time of the first communication" with the individual.

C.4. Recommendations

Recommendation 1

All charities should review their existing fair processing /privacy notices (i.e. information provided at the point personal information is collected) and privacy policies (i.e. further information accessible to individuals about your collection and use of personal information) to ensure they meet the guidance provided in the ICO's ***Privacy Notices, Transparency and Control Code of Practice***.

The information you provide to individuals about how you will use their personal information must be concise, transparent, intelligible and easily accessible. It should also be written in clear and plain language and provide details of their rights and how they can use them.

The methods you use to deliver your fair processing / privacy notices and privacy policies must ensure that there is no ambiguity; individuals must receive sufficient information to enable them to understand what will happened to their personal information so they are able to make informed decisions on whether or not they wish to provide their information and (if you are seeking their consent) provide their consent.

Recommendation 2

All charities should maintain copies of the fair processing / privacy notices and privacy policies they use, with sufficient detail to ensure they know

- The dates during which it was in operation (start date and end date).
- Where it was used (for example, online, application forms, scripts for calls).
- Information about any changes and sign off (i.e. so it is clear which version was in use, and who agreed any changes).

Recommendation 3

Fair processing / privacy notices and privacy policies are the most visible aspect of a charity's approach to Direct Marketing – as they demonstrate what Direct Marketing activities your charity wants to use personal information for (**Section A: Purposes**) and the basis on which you plan to obtain and use personal data – especially which channels of communication you wish to use (**Section B: Lawfulness**).

All charities should therefore ensure their fair processing / privacy notices and privacy policies are reviewed by Trustees as part of the annual review of their approach to Direct Marketing.

Section summary

C. Fairness and Transparency

Suggested actions to take:

1. Define all "data collection points" used by your charity – i.e. the points at which you collect personal information for Direct Marketing purposes (electronically; on paper; face-to-face; verbally).
2. Ensure each "data collection point" contains an agreed fair processing / privacy notice.
3. Ensure your published privacy policy sufficiently addresses data protection and fundraising, including details on your use of personal information for Direct Marketing purposes, the lawfulness of this, and any additional detail required to ensure individuals can understand what will happen to their personal information.

D: Using Third Party Suppliers

This section will help you understand:

- What the law requires and what guidance recommends you do to ensure third party suppliers enable your charity to continue to meet its obligations under the DPA and PECR.
- Some examples of different third party fundraising relationships and how you can ensure compliance in these cases.

Charities may choose to engage a third party supplier to deliver elements of their fundraising activity. Any charity that decides to engage a third party supplier must ensure that these relationships enable their charity to continue to meet its obligations under the DPA and PECR.

Law

DPA Schedule 1, Part II, Paragraphs 11 and 12

The DPA requires Data Controllers (i.e. charities) to comply with the following measures when procuring and engaging Data Processors (third party suppliers).

Procurement – undertake sufficient due diligence

Before selecting a supplier, you should seek details of each supplier's current (and/or proposed) approach to information security and assure yourself that it is sufficient.

"...choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out..."

Once the third party supplier is selected...

Written contract

There must be a written contract between you and the supplier.

"...processing is carried out under a contract...which is made or evidenced in writing..."

Maintain control over personal data

The contract must contain the following elements:

- the supplier must act on your instructions only – for example, not use the personal data for their own purposes; inform you of any planned sub-contracting; assist you in the event of a Subject Access Request.
- a commitment that the security arrangements implemented by the supplier will be no less than those which you would have been required to impose.

The contract should also address:

- access to the supplier's facilities to enable auditing;
- the secure return or secure disposal of personal data at the end of the contract.

"...the processing is carried out under a contract...under which the data processor is to act only on instructions from the data controller..."

Impose equivalent security obligations

"...the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle."

Audit and monitoring

Once the contract is in operation, monitor compliance with the security arrangements.

This may include an audit, or other such assurances (for example, reviewing the audit reports from independent assessors engaged by the supplier).

"...take reasonable steps to ensure compliance with those measures."

ICO Guidance on the use of Cloud Computing

Oct-12, Version 1.1.

The ICO has noted that where third party suppliers offer a "take it or leave it" set of terms and conditions without the opportunity for negotiation, the Data Controller remains responsible for ensuring compliance – i.e. for undertaking due diligence and for satisfying itself that the contract terms and conditions being proposed by the third party supplier are sufficient to meet the needs and fulfil the data protection obligations of the Data Controller. (Para. 51).

D1: Where a third party supplier is the source of data to be used by charity

Example 1 – Fundraising platform provider (eg. Just Giving)

Issue

The personal information is being collected via another organisation – for example, via their website.

You need to ensure individuals are provided with sufficient information in order to know what you want to do with their personal information – but you may not be able to control or define what fair processing / privacy notice information the other organisation provides to the individual.

This may restrict what Direct Marketing purposes you can use the personal information for.

Actions

1. Review what fair processing / privacy notice information the other organisation provides to the individual, to ensure you are aware of what an individual is told about your use of their personal information.
2. Discuss with the other organisation how they will collect personal information.
3. Where possible, require the other organisation to update and/or use your own fair processing / privacy notice.

Example 2 – Buying personal data from a third party

Issue

You are engaging a third party supplier to provide you with personal information which you wish to use for Direct Marketing.

You remain responsible for compliance with the DPA and PECR – i.e. you remain responsible for ensuring that the personal information you are buying meets the fairness and transparency requirements of the DPA, and consent for Direct Marketing has been obtained by the third party supplier.

Direct Marketing Guidance

Version: 2.2 19th May 2016 Paras 176-185

"Organisations buying or renting a marketing list from a list broker or other third party must make rigorous checks to satisfy themselves that the third party obtained the personal data fairly and lawfully, that the individuals understood their details would be passed on for marketing purposes, and that they have the necessary consent."

"Organisations must check how and when consent was obtained, by whom, and what the customer was told. It is not acceptable to rely on assurances of indirect consent without undertaking proper due diligence, to demonstrate consent if challenged."

- *"Reasonable due diligence might include checking the following*
- *Who compiled the list? When? Has it been amended or updated since then?*
- *When was consent obtained?*
- *Who obtained it and in what context?*
- *What method was used – eg was it opt-in or opt-out?*
- *Was the information provided clear and intelligible? How was it provided – for example, was it behind a link, in a footnote, in a pop-up box, in a clear statement next to the opt-in box?*
- *Did it specifically mention texts, emails or automated calls?*
- *Did it list organisations by name, by description, or was the consent for disclosure to any third party?*
- *Has the list been screened against the TPS or other relevant preference services? If so, when?*
- *Has the individual expressed any other preferences – for example, regarding marketing calls or mail?*
- *Has the seller received any complaints?*
- *Is the seller a member of a professional body or accredited in some way?"*

Direct Marketing Guide

Version: 2.2 19th May 2016

Indirect consents

"Organisations need to be particularly careful with indirect consent (i.e. consent given to a third party) for calls, texts or emails. The person must have intended to notify the organisation sending the message that they consent to their messages." (para 103).

Leave.EU case

The ICO noted in this case that Leave.EU *"...relied upon contractual assurances from its third party data supplier that the necessary consent had been obtained for sending unsolicited direct marketing text messages. However, the [ICO] does not consider that [they] undertook sufficient due diligence."*

When asked to investigate the complaints, Leave.EU informed the ICO that their data supplier regarded the data as *"double opt-in consented for government and local government marketing."*

But the ICO concluded this wasn't clear or explicit enough, because it did not mention political campaigning. Stephen Eckersley, ICO Head of Enforcement, said *"the consent wasn't clear. Local and national government was as specific as it got, there was no mention of leaving the EU."*

Example 3 – Data collection

Issue

You are engaging a third party supplier to collect personal information on your behalf.

The third party supplier is acting as an agent of your charity. You remain responsible for compliance with the DPA and PECR – i.e. you remain responsible for the fair and transparent collection of personal information.

Action

Ensure you provide the third party supplier with the fair processing / privacy notice information you want them to use when collecting personal information on your behalf.

This must ensure individuals are clear who the third party supplier is working for, and what will happen to the personal information.

D2: Where a third party supplier uses charity data to provide a service for the charity

Example – Fulfilment

Issue

You are engaging a third party supplier to distribute your Direct Marketing.

This requires you to exchange personal information with the third party supplier. You remain responsible for compliance with the DPA – i.e. you remain responsible for ensuring the security of the personal information, and for how any returns, objections and/or complaints are handled.

Actions

Ensure the contract with the third party supplier includes clauses to address, in addition to the minimum requirements outline above:

- Secure exchange of data with the supplier – i.e. how you will share the personal information with the supplier
- Secure return of data – i.e. what will happen to the personal information once the activity has been completed. This might include the secure return of the information to you, or confirmation of secure disposal by the third party supplier.
- Define who will handle returns (for example, "not at this address")
- Define who will handle objections and/or complaints.

Section Summary

D. Using third party suppliers

Suggested actions to take:

1. Review existing relationships with third party suppliers to ensure each
    a. is based on a written contract.
    b. addresses data protection responsibilities, including purpose and data security.
    c. enables you to manage the personal information throughout the relationship with the supplier, i.e. from the moment personal information is passed to them / collected by them, through until the secure return or disposal of the information.
2. Define a procurement process that ensures sufficient due diligence is undertaken when selecting potential suppliers, and then results in contracts that contain the minimum DPA contract clauses.
3. Define a contract monitoring programme that provides sufficient oversight of the third party supplier's performance. This should include
    a. a reporting process to your charity for any complaints received by the supplier, or about the suplier
    b. an escalation process for serious concerns or breaches of contract to an appropriate level of management within the charity
    c. regular reporting to Trustees on third party supplier performance.

6. Guidance and other Resources

The following additional guidance and resources are available on our website www.fundraisingregulator.org.uk

- Consent self-assessment tool
- Checklist of actions to consider before sending Direct Marketing Communications
- Case Studies from Charities

Other ICO Guidance and Resources

Direct Marketing Guidance: https://ico.org.uk/media/1555/direct-marketing-guidance.pdf

Privacy notices Code of Practice: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

Personal data quick reference guide: https://ico.org.uk/media/for-organisations/documents/1549/determining_what_is_personal_data_quick_reference_guide.pdf

Data Protection self-assessment toolkit: https://ico.org.uk/for-organisations/improve-your-practices/data-protection-self-assessment-toolkit/