Conference paper
21 February 2017

Fundraising and regulatory compliance

Information Commissioner's Office

What's covered

The Data Protection Act 1998 (DPA):

- is based on eight principles of good information handling
- gives individuals specific rights over their personal information, and
- places obligations on organisations that process that information.

In the last 18 months, we've done a series of investigations into the fundraising practices of many charities. We've uncovered practices that seriously violate DPA principles.

This conference paper:

- describes these practices
- says why they contravene the DPA, and
- explains what we think about them.

The conference paper is not just for people working in charities. We'd also like you to read it if you do the kind of fundraising it covers. The conference paper is as relevant to schools and universities as it is to animal welfare and medical charities.

Inside you'll find information about the following things:

- **Wealth screening**
  Analysing donors' personal information to see, for example, whether they might be able to increase their giving.
- **Data matching and teleappending**
  Finding more information about donors – such as their email and postal addresses or phone numbers – which they may not have given you themselves, and adding it to your records.
- **Re-using publicly available information**
  How the DPA applies to information you get from public sources such as the edited electoral roll, Facebook and publicly available registers.
- **How the 'legitimate interest' condition applies to processing**.
- **Fair processing notices**.
- **How the Fundraising Preference Service (FPS) and the Telephone Preference Service (TPS) interact**.

This conference paper doesn't cover your need to get potential donors' effective consent for many fundraising activities. For more about consent, please read our privacy notices code of practice and our direct marketing

guidance. You should also read the Fundraising Regulator's guide to consent. We'll publish our own specific guidance on consent under the General Data Protection Regulation (GDPR) later this year. We'll also produce a new Direct Marketing Code of Practice, which will cover fundraising.

What the law says

The data protection Principles may apply to the first three activities above. Virtually all the activities will raise questions about whether you are complying with Principle 1 of the DPA. Principle 1 imposes separate but related obligations on organisations about how they must process personal information. These are as follows:

- You must process personal information fairly.
- You must process personal information lawfully.
- Data controllers – the organisations in control of processing the data – must have a legitimate basis from within the DPA for processing the personal information.

The points under the next few headings tell you more about these obligations.

Fair processing

Fair processing has two separate aspects:

- You must be transparent with individuals about what you're doing with their data and why.
- You must ensure you process personal information fairly. Broadly, this means you must process it in a way that individuals would reasonably expect.

Being transparent and giving individuals accessible information about how you'll use their personal data is a key part of the DPA and the forthcoming EU General Data Protection Regulation (GDPR). The most common way to give this information is in a **privacy notice**.

For the processing to be fair, the DPA says the data controller must make certain information available to the data subjects (the individuals to whom the data relates), as far as practicable. This information is:

- who the data controller is
- the purposes for which you'll process the information, and
- other information you'll need to enable the processing to be fair in the specific circumstances.

This applies whether you got the personal data directly from the individual or from other sources. Remember that transparency is only one of the two parts of fair processing. A good privacy notice will go some way towards ensuring fair processing and may also help to shape an individual's reasonable expectations. However, a privacy notice isn't enough to make clearly unfair processing fair. You must also consider how the processing affects the individual. Processing does not become fair just because you tell the person it will happen.

This conference paper looks at how the fair processing requirements apply to the fundraising activities that concern us. In particular, it looks at what other information you should give individuals to make the processing fair (the third bullet point above). If you need general advice on how to write a privacy notice or how best to provide one, please consult the ICO privacy notices code of practice.

Lawful processing

In simple terms, the requirement to process personal information lawfully means you must not process it in a way that would break the statute or common law. If processing personal information involves committing a criminal offence, then the processing will obviously be unlawful. However, processing will also be unlawful if it contravenes the common-law duty of confidence or the Human Rights Act 1998, for example.

Basis for processing

This requires organisations to satisfy one of the conditions from schedule 2 of the DPA in order to legitimise their processing of personal data.

If you are processing sensitive personal data, such as information about an individual's physical or mental health, you'll also need to satisfy a condition from schedule 3 of the DPA.

Regarding the schedule 2 conditions, in almost all cases only two conditions relate to fundraising activities. These are:

- whether or not the individual has consented to the processing, and
- whether or not the processing is pursuing a legitimate interest of the data controller or a third party to whom the data are disclosed.

Regarding the schedule 3 conditions, they are highly unlikely to apply except when the data subject has given their explicit consent.

Processing on the basis of legitimate interests

The legitimate interest condition is more complex. It is important for you to know that simply processing for a legitimate interest is not enough to satisfy the condition. If you rely on the legitimate interest condition, you must consider three questions:

- What is your legitimate interest or that of a third party?
- Is the processing of the personal information **necessary** to pursue that legitimate interest?
- Even if it is, would the processing affect the rights and freedoms or legitimate interests of the individual(s) in such a way and to such an extent that it is unjustified?

In simple terms, relying on the legitimate interest condition requires you to carry out a balancing exercise. On the one hand you must consider the legitimate interest you are pursuing and its benefits. On the other, you must consider the potential harm to the rights and freedoms of the individuals whose personal information you are processing. Typically this will involve considering how far the processing infringes their privacy and the effect of that infringement. For the condition to be met, your legitimate interests need not be in harmony with those of the individual. However, if there is a serious mismatch between competing interests, the individual's legitimate interests will come first.

Other principles

The activities detailed in this conference paper also touch on other principles, specifically Principles 2 and 4. You can find more information on how all the principles apply in the ICO Guide to data protection.

Re-use of publicly available information

What is 'publicly available' information?

Many organisations – acting alone or by using third-party data brokers – get and make use of information from the public domain. It often forms the basis of other activities, such as wealth screening or data matching, data cleansing and teleappending/telematching.

The term 'publicly available' can refer to information sourced from various places. It includes information from sources such as the edited version of the electoral roll, as well as being harvested from Facebook pages, Companies House and other publicly accessible sources.

The DPA doesn't stop you getting and using information from publicly available sources. However, you need to ensure that the way you do it complies with all the DPA's requirements.

Put simply, the DPA (Section 27(5)) says you must comply with your duty to give individuals privacy notices unless you satisfy an exemption in the DPA. In other words, even if you've got the personal data from publicly available sources, you must still provide a privacy notice to individuals. It must explain who you are and what you are doing with their data unless you're exempt from that duty.

Don't I only need to supply the information if it's practicable to do so?

As explained above, the DPA requires the organisation processing the personal information to supply information in a privacy notice 'so far as practicable'. In our view if an organisation is able to successfully provide the information required, then it is practicable for it to do so.

The DPA gives several examples of how you might comply with this. It says you must ensure that an individual 'has, is provided with or has made readily available to him' the information required. This gives you some flexibility as to how you give the information to individuals. However, the practicability aspect means you have little room for effectively choosing not to give individuals the information at all.

What about disproportionate effort?

The DPA also suggests you need not give privacy notices if doing so would involve 'disproportionate effort' (which isn't defined in the DPA). One approach to this is to look at whether there's a proportionate balance between the effort involved in giving a privacy notice and the effect of the processing on the individual. In other words, if processing will significantly affect the individual, you should put whatever resources are needed into telling them, but you shouldn't put massive resources into telling people about something that affects them very little. However, if it would be relatively easy for you to inform individuals, you should always do it, even if the effect of the processing on them would not be that great.

Does the fact that the data was publicly available affect what is proportionate?

It may be argued that the fact that the data source is publicly available also affects the balance of what is proportionate. If people assume (or should assume) that their publicly available data can be used for any

purpose, is it proportionate for you to put a lot of effort into telling them how you're using it?

Unfortunately it's not so straightforward and there are several problems with this approach. One problem is that if you have individuals' data and it's feasible to give them a privacy notice – because you have lists of their names and addresses, for example – then you should do so. Also, you shouldn't assume that simply because an individual has put personal information into the public domain, they're agreeing to it being used for any purpose. For example, individuals may want as many people as possible to read their tweet or Facebook post. Yet that doesn't mean they're agreeing to have those pieces of information collected and analysed to set (say) their insurance premium or their credit risk. The fact that personal information is publicly available doesn't make it 'fair game'. And it doesn't make further use of that personal information for any purpose fair.

An individual's reasonable expectations are part of the assessment of whether you are processing personal information fairly. This assessment is separate from the requirement to be transparent with individuals about what you're doing with their personal information and why. The DPA's transparency requirements about what individuals should be told and when are specific and prescriptive. The situations in which you need not comply with these requirements are limited only to those situations where it would be difficult to inform individuals.

Publicly available information and Principle 2

When obtaining and using publicly available personal information, you must ensure you're getting and using it for specified and lawful purposes as required by Principle 2 of the DPA. Further, the purposes for which you intend to process the personal information must be compatible with the purposes for which its processing was originally intended. So when you are getting and intending to use this information, you must compare the original purpose for which it was collected and used against the purpose for which you intend to use it. In deciding whether the two are compatible, you should consider things such as:

- the individuals' reasonable expectations
- the potential effect on them of the processing
- what they've been told.

Many of these factors are the same as or similar to those you would consider in assessing whether processing is fair. That's because the test for assessing compatibility of purpose is broadly similar to the test for assessing fairness.

How this affects other activities

We've dealt with whether information is 'publicly available' first because this can significantly affect whether or not the other activities dealt with in this conference paper comply with the DPA. For example, wealth screening and data cleansing often involve using personal information taken from publicly available sources. If individuals have not been told that their personal information will be used for wealth screening and data cleansing and by whom, the whole operation will contravene Principle 1 of the DPA.

Remember that even if individuals have been told, this won't be enough to make clearly unfair processing fair.

Wealth screening

Wealth screening includes activities such as analysing personal information to assess donors' financial viability. Charities typically do this to see what someone's likely level of donation would be or whether they'd be likely to leave a legacy donation. They may also wealth-screen to establish an individual's 'cross-sell potential' – how likely they would be to donate to other charities. Wealth screening may be done internally or by sharing personal information with third-party companies. Either approach raises several data protection concerns.

Principle 1 issues – fair processing

Wealth screening is the kind of processing that individuals are highly unlikely to expect as a result of their charitable giving. They would not reasonably expect that such a gift would lead the charity to profile their wealth to see whether they'd increase their donations or leave a legacy donation.

So you'll need to inform individuals that you're doing this processing and using their personal information for it. Remember that the purpose of providing a privacy notice is to ensure that individuals have a reasonable understanding of how their personal information will be used and by whom. It's also important because if individuals know the processing is taking place, they can exercise their rights over it, such as the right to object to the processing. If individuals remain unaware, they cannot do this. So how you explain what you're doing with their personal information is important.

A privacy notice should be clear enough for an individual to reasonably foresee how and why you'll use their data. Individuals are unlikely to understand what wealth screening is. So simply stating that you may

analyse their personal information to predict future levels of donation is likely to be too vague. Your privacy notice must be detailed enough to ensure they have a reasonable understanding of what wealth screening is and how you'll use their personal information to do it. If the way you wealth-screen involves disclosing personal information to third parties, you should also make this clear.

How should you tell individuals?

If individuals would not reasonably expect what you'll do with their information, then you need to actively provide privacy information rather than simply making it available for them to look for themselves, for example on your website. So if you intend to process personal information for wealth screening, you should actively communicate this to individuals. Often the easiest way will be to tell them at the point when you first collect their details.

Principle 1 issues – basis for processing

You must also ensure you have a valid basis for the processing. It's legitimate for you to process personal data in order to properly administer donations received from individuals. However, processing personal data for wealth screening isn't **necessary** in order for you to do this. In other words, charities and other fundraising bodies cannot include wealth screening as part of their legitimate interest in administering donations.

Wealth screening is a separate and distinct activity that requires its own basis for processing from within the DPA. It may be argued that wealth screening is itself a legitimate activity by fundraisers. However, you must consider the privacy intrusion in wealth screening. Individuals may well wish to donate to a charity. But they may not want their personal data analysed and profiled to assess how much they could donate.

Wealth screening may cover a broad spectrum of activities. These could range from simply segmenting your donor database by postcode, through to using dedicated third-party companies to obtain more personal information and generate donor profiles. Given the broad range of activities wealth screening can include and the different levels of intrusion they represent, the legitimate interest condition is unlikely to cover all the activities that may be considered wealth screening.

Activities such as segmenting databases by reference to postcodes or other information you already have may represent a relatively low level of intrusion into privacy. In these cases, the legitimate interest condition may be a valid basis for processing. Far more intrusive are activities such as profiling individuals, particularly where this involves getting more

information that the individual has not given you, either directly or via third-party companies. In these cases the legitimate interest condition is highly unlikely to apply. So you'd need to seek the consent of individuals before doing such processing. It follows that there is an element of risk in relying on the legitimate interest condition for wealth screening. For more certainty you should seek the individual's consent.

Some organisations use personal information from publicly available sources as part of their wealth screening. This will contravene Principle 1 of the DPA if you have got or used the information in a way that breaches the DPA or any other law, even if you got or obtained it from another party or they are wealth-screening for you. See the earlier section on 're-use of publicly available information' for more information.

Principle 2 issues – incompatible purposes

The DPA requires that personal information is obtained for specified and lawful purposes. You must not use it in a way that's incompatible with the initial purposes for which it was obtained. As explained above, wealth screening would be outside what individuals would reasonably expect you to use their personal information for after they've donated. So wealth screening is incompatible with the purpose of administering donations. Failing to specify wealth screening as a purpose for processing also breaches Principle 2 of the DPA.

Data matching and teleappending

Data matching and teleappending are activities that involve obtaining personal data from other sources which individuals did not give you when you initially collected their personal information. It's also sometimes called data cleansing. Examples include:

- getting a phone number or email address from a website or some other source
- getting postal addresses if you find that an individual has moved and no longer lives at the address you have on file.

Regardless of where you get this information, unless you return to the data subject and obtain it from them, this type of processing will be unfair in most cases. This is likely be true no matter how clearly you explain it to them, because it removes the data subject's choice about what information you hold about them.

Individuals may have deliberately withheld certain information from you, such as email addresses and phone numbers, because they don't want to receive marketing via these channels. By getting that information from

other sources, you'll be going directly against their wishes. Individuals wouldn't reasonably expect you to contact them using details they never gave you.

It could be argued that individuals may have forgotten to give you the information or update you about moving house, for example. But you cannot assume this is true. Even if they've forgotten, they still wouldn't reasonably expect you to contact them via a phone number or email address they never gave you.

So is data matching and teleappending never ok?

You may be able to use data for data matching and teleappending if you're satisfied that the data source is legitimate and the individual had a clear, legitimate expectation that their details would be passed on for this purpose. For example, an individual may have moved house and made clear to the data source, by ticking a box or some other positive action, that they wanted them to inform third parties of the change of address. However, if there's no evidence of such an expectation, the processing is highly likely to be unfair.

But don't we have to keep our personal information up to date?

Some argue that data matching and teleappending is needed to enable them to comply with the requirement, under Principle 4 of the DPA, to keep their personal data accurate and up to date. However, you can meet this requirement without using such methods. If you find that an individual has moved house, you should update your records to reflect that. This will be enough to comply with Principle 4; you don't need to seek out their new address.

Interaction between the Fundraising Preference Service (FPS) and the Telephone Preference Service (TPS)

What are the TPS and the FPS?

In our view, fundraising calls, texts and emails fall within the definition of direct marketing found in the DPA. For more information, see the ICO Direct Marketing Guidance. Also, all references in this conference paper to the FPS refer to the Fundraising Preference Service. This should not be confused with the Fax Preference Service, which the conference paper does not deal with.

The FPS and TPS are registers that individuals can choose to be included in. By opting to be included in the FPS or TPS (or both), individuals are objecting to receiving direct marketing communications. Registering on the TPS represents a general objection to receiving direct marketing communications via live telephone calls. Organisations should not make such calls to numbers registered on the TPS unless they have received prior consent to do so. However, if they do have consent to make live marketing calls to an individual, the fact that the person later registers their number with the TPS will not override that prior consent.

In contrast, registering on the FPS is a specific objection to receiving direct marketing communications, including live fundraising calls, from specific charities or types of charities. The FPS is intended to be a reset button. So inclusion on it would invalidate any consent to marketing that the individual had previously given.

This may have led to some confusion about how the two registers interact, particularly because the TPS is a statutory register, set up via the Privacy & Electronic Communications Regulations 2003 (PECR), while the FPS has no such statutory footing. Further, organisations must screen their call lists against the TPS but there is no such duty to screen against the FPS.

In our view, you should regard the FPS as acting on behalf of or as an agent for subscribers who wish to withdraw their consent or object to being contacted by particular bodies – it's not a general objection to receiving direct marketing calls. Because it's a clear and specific objection to a particular type of call from particular organisations or types of organisations, you should not call that number – regardless of whether it's registered on the TPS or whether you had prior consent to call – as soon as you're aware the number is registered. FPS registration overrides any prior consent you may have received to make marketing calls to the individual. This includes any prior consent you may have relied on to circumvent the fact that the number was registered on the TPS.

The information in this document is intended for use as a conference paper at this Fundraising & Regulatory Compliance event. It represents the ICO's current position at this time but will not be updated or amended. For our most up-to-date guidance on data protection and freedom of information issues, you should consult the guidance index on our website, ico.org.uk.