

More

Consent, Opt-In, Legitimate Interest and GDPR

This article is a discussion of questions about whether or not organisations should, or are compelled to, adopt an “opt-in only” approach for managing their supporter, alumni, member or ticket buyer databases under GDPR.

If you are connected with a charity that receives state funding (like a university, publicly-funded museum, state school or any other organisation subject to the Freedom of Information Act), then you also need to read the article I have written on Public Authorities. There are important differences relating to the use of Legitimate Interest for these organisations.

Grounds for Lawful Processing

It's a basic building block of Data Protection legislation that a Data Controller must have one or more legal justification for processing someone's data. This is called the “ground for lawful processing.” Under GDPR there will be six of these, of which the two most relevant for charities are “Consent” (Article 6.1.a) and the “Legitimate Interests” of the data controller (Article 6.1.f).ⁱ This is not greatly different from the current Data Protection Act, although the standard for consent is raised under GDPR, as is the standard of the test necessary for processing under Legitimate Interests.

The fundamental difference between Consent and Legitimate Interest is as follows:

- Consent: “Here's what we would like to do with your data. We will only do it if you tell us it's OK.”
- Legitimate Interest: “Here's what we intend to do with your data. We need to do it, we don't believe it will harm you. You can tell us you'd prefer us not to.”

Under the existing Data Protection Act, the fundraising and supporter relations function in many charities and most universities and schools is likely to have been relying on “Legitimate Interest” to make the basic business of holding people's information lawful. This ground for processing is important since it is unlikely that the organisation has formal, auditable consent from each person who is on their database.

This should not be confused with the absolute requirement to have consent to send direct marketing by email or SMS, or to telephone TPS registered numbers. This is a result of the Privacy and Electronic Communications Regulations which are additional to the Data Protection Act and GDPR. So “Legitimate Interest” might make it lawful to have someone's email address on your database for admin purposes, but you'd need consent to use it for marketing purposes.

Fundraising Consultants. And More.

What is the implication of using Consent (or Opt-In) only?

The spotlight on the fundraising world over the last 24 months has pushed many charities to decide only to process people's data if they have formal, auditable consent. The shorthand name that has been used for this is "opt-in only" but really it is about consent. Deciding to go to "opt-in only" is, in effect, a voluntary decision to use consent (freely given, informed, specific consent) as their only ground for lawful processing.ⁱⁱ

Organisations which choose to take this route are likely to end up with a much smaller core of very committed supporters, since "opt-in only" will require them to stop processing data for anyone who does not respond to a request for consent to process data.ⁱⁱⁱ

On the positive side, Consent means that the charity knows that it is ok to process the individual's data and has the confidence that the individual knows and is happy with what will be done with it. This is why some say that Consent is the "safest" way of processing people's data. The chance of regulatory action is very low indeed. If someone complains about the way their data is being used, the response would be "but we explained to you what we do with your data and you told us we could." This is why ICO and the Fundraising Regulator like Consent so much.

But even the Information Commissioner's Office themselves have said that consent is not always appropriate or easy to obtain. And it may be that organisations do not want to risk the significant attrition that will come from relying on consent as the only ground for processing.

This is especially the case for those whose relationship with an organisation is a lifelong one which may mature and develop as time goes on. At the age of 22, it may be that Facebook and WhatsApp are all that's needed to keep in touch with University friends, and a core connection with the university itself seems unnecessary. By the age of 40 this may have changed. But by this point, on a Consent-only model, the university and the alum may well have lost touch and so the former student will be unable to receive what might have been a welcome invitation to re-engage, come to an event or support an initiative. The same could be said of connections between supporters and causes related to life-defining events, like the illness or death of a close friend or relative, and of deeply held political, social or religious convictions.

Identifying potential donors

Many charities now have established relationships with major donors, and others are setting up major gifts functions. This form of fundraising relies on considerable depth of relationship between charity and donor. While a small number of charities have received entirely unsolicited large gifts, most do not and they are few and far between. For this reason, "consent-only" is not logically possible in this realm of fundraising. Potential donors have to be identified.

Major gifts fundraising relies on the ability to approach someone who may be interested in a cause, and to give them opportunities to find out if this is correct. You can't ask someone for consent before you've communicated with them, let alone worked out who they are. Major Gifts fundraising will always rely, at least to an extent, on something other than pre-gathered consent.

So, if not Consent, what about Legitimate Interest?

Remember that under Legitimate Interest, an organisation is saying “Here’s what we intend to do with your data. You can tell us if you’d prefer us not to.” So how do you do that? A good privacy notice is essential, but additionally, GDPR will require an organisation which relies on Legitimate Interest to ensure that the processing is necessary, and that the organisation’s interests are not overridden by *“the interests or fundamental rights and freedoms of the data subject which require protection of personal data.”* GDPR Recital 47 provides more information. This is a more testing requirement than under the Data Protection Act, but the same recital goes on to suggest that circumstances under which this might be reasonable include *“where there is a relevant and appropriate relationship between the data subject and the controller...”* The recital is clear that direct marketing can be carried out as a legitimate interest.

So how would you judge whether or not you’ve upheld a person’s interests or fundamental rights and freedoms? The ICO provides information about how to conduct a Privacy Impact Assessment (PIA), which is an optional but robust way of making this judgement. Another important criterion is to ask whether or not the person is expecting the kind of processing which you say is in your Legitimate Interest. There is plenty of evidence to show that high net worth individuals are not surprised to be approached by charities, and indeed are put off by naïve, ill-prepared approaches.^{iv} And, once again, your case will be significantly enhanced if your rationale for processing is documented.

Bear in mind that your interest and those of the data subject do not have to align. ICO quotes the legitimate example of a debt collection agency using Legitimate Interest as the ground for processing as they pursue a debtor who has interests which are manifestly not aligned with that of the agency!^v

When can’t we use Legitimate Interest?

You can’t use Legitimate Interest to make marketing telephone calls to TPS-registered phone numbers, and you can’t use it to send marketing emails and SMS messages at all. You need consent to do this.

You’d also need consent if you were going to do something people wouldn’t expect. So if you wanted to share your data with another charity or sell it to someone, then unless you could show people expected it and they knew about it, you’d need consent.

You also need consent to process certain categories of sensitive data – religious and political affiliation, sexual orientation and health information and so on. Here, legitimate interest is not enough. Some people think that financial information is sensitive. While ICO has argued that collecting financial information is intrusive, it is not, in law, classified as sensitive.

So, can’t we just keep on relying on Legitimate Interest and ignore all this stuff about “Opt-In”?

There will be times when it’s OK to rely on legitimate interest and times when it won’t be. If you are doing something the person didn’t know you were doing and wouldn’t expect, and especially if you thought they would be upset by it, then you shouldn’t rely on legitimate interest. But if your privacy notice is in order, and you know you’ve communicated it to people and can show that you’ve thought about how you’ve balanced your needs and

legitimate interest with the “*interests and fundamental rights*” of the data subject, then in many circumstances you should be able to.

What about Prospect Research and Wealth Screening?

An argument might go as follows: you have told people in your privacy statement that you will be using their data to wealth screen and do prospect research, since this will serve the needs of the charity, ensure that the communication and approaches they receive will be appropriate to them and you’ve judged that it will not cause them harm. You’ve made it clear how they can ask you not to do this. You’ve backed this up with a written Privacy Impact Assessment, which showed that the change in your fundraising behaviour towards 98% of the people you wealth screen will be zero (since they won’t match a wealth screen), and the 2% where your fundraising behaviour is changed would not be surprised at this. This seems to me to fit all the criteria for lawful processing under the Legitimate Interest ground for processing. You need to do it, and they know about it, can opt-out and are not harmed by it.

However, this still doesn’t address ICO’s assertion in their paper for the 21 February 2017 conference that Principle 2 may be breached by using data from, for example, Companies House or from Twitter. They argue this is beyond people’s expectation, because data use by the charity is a different purpose than the one for which the information was put in the public domain, on Companies House or Twitter. Therefore, ICO argues, the provision of a privacy notice by the charity doesn’t make fair that which they regard as inherently unfair. However, this assertion must be seen in the context of Twitter’s own privacy policy which says “*What you share on Twitter may be viewed all around the world instantly. You are what you Tweet!*”. So the question is, would company officers or Twitter users be surprised that the publicly available information at Companies House or on Twitter has been read and used by a charity doing respectful prospect research? If the answer is “yes” then the processing may breach Principle 2. If the answer is “No” then it probably doesn’t.

Where does this leave us?

Unless what you are doing is wholly unexpected by the data subject, there doesn’t seem to be any compelling generic reason for choosing “Consent” as your ground for lawful processing of your core supporter/alumni/member/ticket-buyer database. This same point has been argued also by Ken Burnett on the 7th April in the 101 Fundraising blog.^{vi}

I also believe that Legitimate Interest should provide grounds for lawful processing in respect of Prospect Research, and probably wealth screening as well. But I know I am at odds with the Information Commissioner on the latter at least.

So, what to do?

- Carry out Privacy Impact Assessments. They are a methodological way of looking at what processing happens and its impact on people.
- Revise Privacy Notices and make them as full as reasonably possible, and written in a way which explains what processing is all about.
- Read Tim Turner’s excellent guidance on Fundraising and Data Protection. Tim runs a blog in which he makes his views about privacy law very clear. He has been very critical of charities in the recent past and has engaged in, let’s say, a robust fashion on Twitter with those including me who sought to defend them. But his explanation of the way the law works is second to none, and where he disagrees with the Information Commissioner,

he's not afraid to say so. His guide is here <http://2040training.co.uk/wp-content/uploads/2017/03/Fundraising-DP-guide.pdf>. If it helps you, please do as Tim asks and make a gift to a mental health charity.

As always, this is not legal advice. I'm simply a fundraiser who's spent a lot of time thinking about data protection. If in doubt, you or your organisation should, take legal advice.

Adrian Beney, More Partnership

7 April 2017

ⁱ For membership processing or the sale of tickets, "processing necessary for the performance of a contract", Article 6.1.b may also apply to that process, but it probably does not apply to fundraising from the same people.

ⁱⁱ The Fundraising Regulator's guidance makes this clear. See p 35, Recommendation 2 OF <https://www.fundraisingregulator.org.uk/wp-content/uploads/2017/02/GuidanceFinal.pdf>

ⁱⁱⁱ The RNLI's contactable database has reduced from around 2.1 million people to around 600,000.

^{iv} See upcoming research from Dr Beth Breeze for the Institute of Fundraising.

^v <https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/> under "What is the legitimate interests condition?"

^{vi} <http://101fundraising.org/2017/04/opt-will-bad-donors-bad-causes-support/>