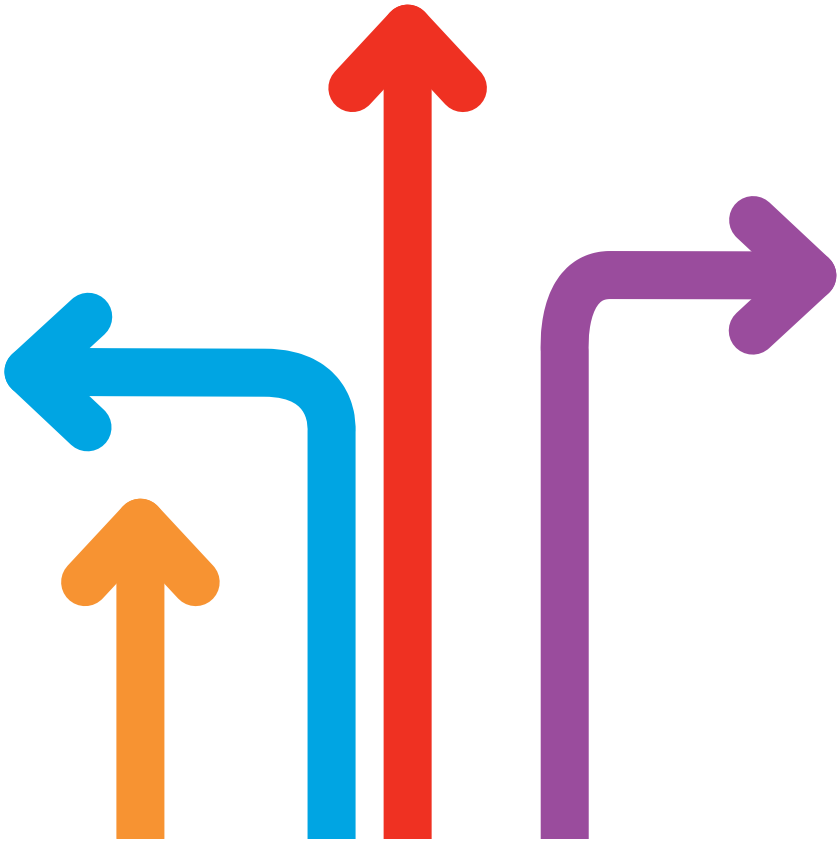
Institute of Fundraising

In partnership with

BDB PITMANS



GDPR:
THE ESSENTIALS FOR FUNDRAISING ORGANISATIONS

Version 2. March 2019

About the Institute of Fundraising

The Institute of Fundraising (IoF) is the professional membership body for UK fundraising. We support fundraisers through leadership and representation; best practice and compliance; education and networking; and we champion and promote fundraising as a career choice. We have over 600 organisational members who raise more than £10 billion in income for good causes every year, and over 6,000 individual members.

www.institute-of-fundraising.org.uk

About BDB Pitmans

BDB Pitmans is an award winning, top 60 UK law firm with offices in London, Cambridge, Reading and Southampton. Many of the lawyers and advisers are recognised leaders in their practice areas – their knowledge and expertise helps us to provide a unique, client centred approach to law.

Our success has been built through developing long-standing relationships. We listen to you and your business objectives or life goals so that we provide not only excellent technical advice, but a complete solution. We work with you to understand the challenges you face, and aim to not just meet expectations, but to exceed them.

www.bdbpitmans.com

ABOUT THIS GUIDE

On 25 May 2018 the new General Data Protection Regulation (GDPR) came into effect in the UK. This replaced the Data Protection Act (1998) and introduced new and different requirements for all sectors and organisations. Charities, alongside any private sector organisations, business, or public bodies, have to follow these legal requirements when processing individuals' personal data.

There are some key questions which charities need to consider and answer for themselves to ensure they are following the requirements of the law: What are my responsibilities in handling personal data of supporters? How and when can I contact supporters? Do I need to get consent for all communications? What policies and procedures should we have in place?

We have put together this guide to answer those key questions. We know that all fundraisers and charities want to get this right and be sure that they're meeting their legal requirements, as well as giving their donors a great experience of supporting their cause – keeping them up to date with the work of the charity and giving them opportunities to support or be involved in the future.

This guide is for you if:

- You are a fundraiser
- You are a CEO or director responsible for fundraising activities
- You are a trustee of a fundraising organisation
- You don't work as a fundraiser but want to know the basics of GDPR

GDPR covers all organisations, no matter how big or small your organisation or what sector you work in. So, if you are working in a charity that fundraises and takes donations from members of the public, this guide is for you!

What's in this guide and what isn't

This guide is a starting point for fundraisers to be aware of some key areas that they need to be thinking about. It isn't a guide to everything under GDPR but looks at the main issues on direct marketing that our members and the wider fundraising community need to be aware of.

Charities and fundraisers should know that GDPR covers much more than the areas we are able to highlight here – for example, how to keep data safe and secure, and appropriately recording sensitive personal data of service users.

For further information on and the changes introduced by the GDPR we encourage all fundraising organisations to review the guidance given by the Information Commissioner's Office (ICO) www.ico.org.uk

There is also more detailed guidance by the Fundraising Regulator on the use of personal data in fundraising available at www.fundraisingregulator.org.uk

PART ONE
GETTING TO GRIPS WITH THE BASICS

What is GDPR?

The General Data Protection Regulation is an EU-wide regulation which came into effect in the UK on 25 May 2018. It replaced the previous law we had on data protection (the Data Protection Act 1998) and gives individuals more rights and protection in how their personal data is used by organisations.

The GDPR works alongside two other pieces of legislation controlling the use of information:

- The Data Protection Act 2018 supplements the GDPR with some additional rules and exceptions.
- The Privacy and Electronic Communications Regulation 2003 set specific rules on direct marketing.

For simplicity this guide deals with the combined effect of the GDPR and these two other pieces of legislation, without going into detail about which rules come from which piece of legislation.

Are the rules the same for everyone?

Yes, pretty much. Apart from a few exceptions, charities have to abide by the same rules as other sectors and other businesses.

We didn't know about the changes that came in for May 2018, we've taken steps towards GDPR compliance but what happens if we aren't fully compliant yet?

All organisations are expected to be working towards GDPR compliance, and it's your responsibility to be up to date with your legal obligations. The Information Commissioner's Office (ICO) has been clear that compliance is an ongoing task – you should be making steps as soon as you can to be working consistently with the legislation. Compliance with GDPR isn't optional! Get an action plan together to take the steps you need in order to be following the rules.

How do the legal rules and GDPR work with the Fundraising Regulator and the Code of Fundraising Practice?

The Information Commissioner's Office (ICO) regulates data protection laws in the UK. They set the guidance for all sectors and will take complaints and enforcement action where the law has been broken.

The Fundraising Regulator is the independent regulator of fundraising. They set the Code of Fundraising Practice, which includes both relevant law, and standards set by the Fundraising Regulator. The Code has been updated to include relevant information and signposting about GDPR.

It's worth remembering that the Fundraising Regulator can also set rules for fundraisers that go above and beyond what the law sets out, so you should always refer to the Code of Fundraising Practice so that you can be sure you are reaching the standards expected of fundraising organisations.

The main focus of this guide is around the rules on 'direct marketing'. We do fundraising, is that the same thing?

Yes. Legally, direct marketing means directing any advertising or marketing material towards particular individuals. The ICO has issued guidance stating that 'advertising or marketing material' includes any material, which promotes the aims and objectives of the organisation, not just promoting products or services. So, if you are a charity and are using supporters' contact details to keep

in touch with them about fundraising campaigns or news about the charity's work, you are doing direct marketing!

What activities does the GDPR cover in relation to 'direct marketing'?

It applies whenever you collect and use an individual's personal data – including their name, contact details, and any other information about them (even if you are just holding the information on your database). That includes writing to someone, sending him or her an email, or calling him or her on the phone.

The rules don't apply where you aren't using 'personal' information, for example if you were sending material to 'the home owner' rather than using an individual's name and address.

At a glance: communicating through different channels

Remember, that there are some forms of communication, and some type of processing of data, that always require you to have consent. You need consent to send direct marketing by:

- Email to email addresses owned by individuals;
- SMS;
- making automated telephone calls; or
- making telephone calls to individuals who are on the Telephone Preference Service (TPS).

Legitimate interest is only a lawful condition for sending direct marketing by post, or for live calls to telephone numbers not on the TPS, or by email to email addresses owned by corporate bodies.

It is not always easy to tell whether an email address is owned by a corporate body. For example, many trusts are not corporate bodies even if the trustees' email addresses use the name of the trust. If in doubt, the safest approach is to treat the email address like an individual's email, and only send the message if you have consent.

Q. Can I send direct marketing to an individual by post?
A. Yes, if:
1. that individual has given their consent by taking a positive action to opt in; or
2. you are relying on your organisation's 'legitimate interest' and have given individuals the chance to opt out.

Q. Can I send direct marketing by email or SMS to an individual?
A. Only if that individual has given their consent by taking a positive action to opt in.

Q. Can I contact an individual by telephone for marketing purposes?
A. Yes, provided that this is a live (person to person) call and the person has not opted-out of telephone marketing either by contacting you direct or via the Telephone Preference Service. **BUT –** you cannot make automated calls without explicit (opt-in) consent.

Top tips for compliance:

- ✓ Work out who in your organisation will take the lead on this (or get a team together). If you are a smaller organisation this might be harder as you probably won't have a dedicated compliance officer or any in-house legal support. But you do need to think through who is going to be responsible for making sure your organisation is putting in place any changes you need.

- ✓ Remember, GDPR doesn't just apply to fundraising. It applies whenever your organisation is processing personal data of individuals. So that includes campaigns, volunteering, or service user information. It's worth discussing this with your senior management team and trustees so that you have an organisation-wide strategy. Bring in your IT team or the people that work on your databases too.

- ✓ Make the right decisions, not the first decision. It's really important that you think carefully about a decision, which could well have long-term impact for your charity and supporters. While there are some things that you will need to just get on and do, there are other issues where there's some choice for organisations. That's particularly true when thinking about how you will be contacting supporters in the future.

- ✓ A whole organisation approach is necessary with a strategy agreed at Board level. You will need to have documented processes and procedures in place for using and protecting personal data, with support from your executive/board for implementation, monitoring and enforcement: it must never be just down to each fundraiser to make quick decisions by themselves.

- ✓ Think about compliance as an ongoing project – not something that is a time-limited project with a definite end. Like owning a car, it needs regular servicing, and an MOT so it doesn't break down!

PART TWO
‘OPT IN’ CONSENT VS ‘OPT OUT’ – WHAT’S GOING ON?!

Do we need to go 'opt in' for all of our direct marketing to comply with GDPR?

No. GDPR does not require that all direct marketing needs an 'opt in'. That's because there are different legal conditions that you can use to send direct marketing by post, and also different rules for communication by difference channels (see the 'At a glance' boxes above for information on where opt in consent is required).

Remember that not all communications you send will be 'direct marketing'. If you are sending a communication for a genuine administrative purpose, unconnected with direct marketing, the rules for direct marketing don't apply. For more on the definition of 'direct marketing' (which will include all fundraising communications or material promoting the values of the organisation) take a look at the ICO's Direct Marketing Guidance https://ico.org.uk/for-organisations/marketing/

GDPR and consent – the 'opt in' approach

Organisations can send direct marketing/ fundraising materials to an individual where you have consent. Under GDPR the standard of what counts as consent is raised from what was required under the old rules. Essentially, to get consent from an individual for direct marketing under the GDPR, you must have some form of unambiguous positive action that shows that the person is happy to receive those future communications. That action has to be separate or additional to the act of donating. So, consent means that the individual has taken some some form of positive action to 'opt in'.

What counts as a positive opt in?

It could be a tick box approach where people show their consent by ticking a box on a donation form, or it could be choosing between a 'yes/no' option. It could also be an act of supplying your contact details on a form or online provided it is absolutely clear that you are doing so in order to receive direct marketing. It doesn't have to be written down: consent, can be given orally or by a clear action of an individual – for example, putting a business card in a bowl at an event where it is clear that is how they can give their contact details to hear more about the charity.

You don't always need consent to send direct marketing – you could use a different legal condition to process the data and have an 'opt out' mechanism

This is where it gets a bit confusing! Under the GDPR there are different 'legal conditions' through which you can send direct marketing to an individual. One of them is consent, which we've just talked about above. But there is also one called 'legitimate interest' which enables you, in certain circumstances, to be able to send direct marketing to an individual without having their prior consent. But, if you use legitimate interest you will also need to have made sure that they have the opportunity to say 'no' or object to future direct marketing, which is often done through an 'opt out' tick box.

Legitimate interest is the most flexible of the lawful bases for data requests, but it also requires the most thought because you have to assess whether you have a 'legitimate interest' and whether that is outweighed by the interests of the individuals. You should conduct a legitimate interests assessment (LIA) and keep a record of it, which will help to show that you thought about your decisions and can justify them.

The ICO has published guidance about legitimate interests assessments, including a template, here:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

Consent checklist from the Information Commissioner's Office

1. We have checked that consent is the most appropriate lawful basis for processing.
2. We have made the request for consent prominent and separate from our terms and conditions.
3. We ask people to positively opt in.
4. We don't use pre-ticked boxes or any other type of default consent.
5. We use clear, plain language that is easy to understand.
6. We specify why we want the data and what we're going to do with it.
7. We give separate distinct ('granular') options to consent separately to different purposes and types of processing.
8. We name our organisation and any third party controllers who will be relying on the consent.
9. We tell individuals they can withdraw their consent.
10. We ensure that individuals can refuse to consent without detriment.
11. We avoid making consent a precondition of a service.
12. If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

Ok....I haven't heard about legitimate interest before. How does it work?

Organisations can lawfully send direct marketing by post, or make 'live' calls to people who have not objected or registered with the TPS, or send emails to email addresses owned by corporate bodies where:

- there is a legitimate interest AND
- the legitimate interest is not overridden by the rights and interests of the individual.

GDPR text says:

"The processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data..."

It makes clear that *"The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest." (Recital 47)*

This means that direct marketing can be a legitimate interest, but it will not always be. You must consider what the individual would reasonably have expected their personal information to be used for at the time that they provided it. If the individual had not expected the information to be used for direct marketing, it would not be legitimate for the organisation to do so.

You should be considering how to ensure that individuals are given clear information when their details are being collected, so that they know how their personal data will be used. If the information was collected for a different purpose, or if the individual was not informed that the information would be used for direct marketing, you cannot rely on the legitimate interest's condition.

It's also worth thinking through the expectations of your supporters generally and gathering evidence and insight too. If you have donor panels or satisfaction surveys, then it's a good idea to ask supporters about whether they are happy with your communications. That will help not only to give them a better experience, but will also help you understand the reasonable expectations of supporters. Of course, different people will have different expectations so there are likely to be a range of views to consider. You can manage these expectations by effective use of your privacy notice.

So, direct marketing can be in the legitimate interests of a charity, and this can provide a lawful condition for processing an individual's data where you don't have prior consent. But, that's not the end of the story, there's more to know about 'legitimate interest.'

You must consider whether the individual's rights and interests override your charity's legitimate interests in sending the material.

Just like the previous law, the GDPR gives individuals the right to require organisations not to use their personal information for direct marketing. The GDPR is very clear that **the individual's choice to say 'no' to direct marketing is more important than your charity's (legitimate) desire to send them future communications.** If an individual has told the charity that they do not want to receive direct marketing, the charity must not send it.

Where an individual has objected, the position is quite clear, but in other situations it will require more careful thought.

Essentially, legitimate interest becomes a balancing exercise. If you want to use the condition then you should consider your rationale carefully, be able to justify it, and demonstrate that you aren't overriding an individual's rights and that processing the data to send direct marketing is within their reasonable expectations. The way to do this would be to carry out a legitimate interests assessment and to give thought to the individual's rights and expectations.

The example in the table below gives an illustration of how you might go about this, although it must be made clear that legitimate interest must be assessed on a case by case basis by each organisation.

How you could carry out a balancing exercise on your legitimate interests

Processing of an individual's data	Do we have a legitimate interest, taking account of the individual's reasonable expectations?	Are we sure we aren't overriding their fundamental rights?	Are we confident we pass the legitimate interest test?
1. We would like to send by post a newsletter with information on our work and our latest fundraising appeal to an individual who has donated to us last year.	Yes, we have a legitimate interest. The GDPR is clear that direct marketing may be considered a legitimate interest. Sending the newsletter and the appeal is direct marketing. The individual would reasonably expect us to send the material because: • this is an individual who has donated to us in the recent past; • when we collected their data for the previous donation we gave them clear information in our privacy notice that we would send them direct marketing in the future; and • We gave them a clear opportunity to object by 'opting out', and they did not do so.	Yes, we are sure. The individual has not objected to receiving direct marketing. The material we want to send is not intrusive, and there are no other reasons to believe the individual would rather not receive it.	Yes

Processing of an individual's data	Do we have a legitimate interest, taking account of the individual's reasonable expectations?	Are we sure we aren't overriding their fundamental rights?	Are we confident we pass the legitimate interest test?
2. We want to send our Christmas appeal to an individual who has donated to us in the past, but see that they've called us 6 months ago and said they don't want any further marketing.	Direct marketing can be a legitimate interest. At the time we collected the information we made clear that it would be used for direct marketing and the individual did not opt out when given the opportunity. However, the individual's reasonable expectations will have changed now that we have been asked not to send further direct marketing.	No. The individual has exercised their right to object to direct marketing, and that overrides our interests in sending it to them.	No. The individual's rights and interests override ours.
3. We have people who have given us cash donations over time but we haven't had a donation from them in the last 2 years. Can we send them our next newsletter and fundraising appeal by post?	Again, direct marketing can be a legitimate interest. However, we need to consider the reasonable expectations of the individual. This will require us to think through a number of issues; for example, we will need to check our privacy policy and past communications as to whether the individual was given a choice about future marketing, were they given an 'opt out' option previously, and are we satisfied that they had a reasonable understanding of how their data would be used? Would that individual be surprised to receive this mailing? What does our data retention policy say about 'dormant' or 'lapsed' donors? The Fundraising Regulator has produced a useful self-assessment tool to help you understand the key aspects to think through and identify where any risks lie: https://www.fundraisingregulator.org.uk/wp-content/uploads/2017/02/ConsentSelf-AssessmentToolFinal.pdf	If we decide we do not have a legitimate interest, we do not need to consider the next part of the test. Otherwise, as the Fundraising Regulator says, this will only be able to be judged on a case by case basis. We will need to weigh up the factors, and be confident that our organisation's legitimate interest is not overriding an individual's privacy rights.	Maybe. As indicated, if we decide that we have a legitimate interest, it will be a question of whether we are confident that our organisation's legitimate interest is not overriding an individual's privacy rights – if we aren't confident, then don't send it.

Is having a legitimate interest sufficient in itself for justifying direct marketing?

Having a legitimate interest may not be sufficient in itself if there are better alternative options for obtaining information. You can only rely on the legitimate interests condition if the activity you are planning is necessary in order to achieve your legitimate interest. You should consider the necessity of processing data using the legitimate interest justification.

ICO Necessity Test

Consider:

- Does this processing actually help to further that interest?
- Is it a proportionate way of achieving your purpose?
- Could you achieve the purpose without using the data, or by using less of it?
- Is there another less intrusive way to achieve the same result?

So, what should I do at my charity? Should we change to only send direct marketing when we have consent and go 'opt in', or should we keep using an 'opt out' and rely on our legitimate interest?

This is really where it is a choice for your charity, based on a whole number of factors including your fundraising strategy, the size of your organisation, and considering who your donors and supporters are. Think through the range of options that are available. There might be consideration too of a more nuanced approach, where you seek consent for some channels (email and text), but not for direct mail where you decide to rely on your legitimate interest.

Some larger national organisations have publicly announced that they are moving to 'opt in' for all communications as they have decided that's the strategy that will work best for them. But others are choosing the alternative 'opt out' approach.

You are going to have to decide the right approach for your charity. Be aware of all the relevant factors, including how any changes might impact your income and operations in the short, medium, and long term. Also, consider the interplay between the range of communications you send and how fundraising fits in with wider marketing that your charity does. These are really important issues, which is why it's important to ensure that you take sufficient time to make the right decision, adopt a 'whole organisation' approach, and also ensure that trustees are involved appropriately in strategic decisions.

Whatever approach you take, you must ensure that your privacy notices are clear about what information you collect and how you will use it.

What does the IoF say?

We do not believe that a one size fits all approach is appropriate. Consent (opt in) will be right for some charities, relying on your legitimate interest (opt out) will be right for others. The most important thing is that whichever you choose to rely on, your donors and supporters are being treated fairly and respectfully and that you are meeting your legal obligations. Both 'opt in' and 'opt out' can be done well in giving your supporters an excellent experience of your charity and in building long-term positive relationships.

To 'opt in' or to 'opt out':

This is potentially the most important strategic decision that your charity can make in terms of your direct marketing practice. Here are our tips on how to go about coming to a decision.

- ✓ Make sure you really understand the rules and what both Consent and Legitimate Interest require.
- ✓ Review the relevant guidance from the Fundraising Regulator and the ICO.
- ✓ Adopt a 'whole organisation' approach that brings in other teams and departments. Are all the right people involved in the decision – finance teams, campaigns, IT, and of course, the trustees?
- ✓ Update your privacy notice to explain clearly what information you collect and how you use it.
- ✓ Consider whether associated policies (e.g. a data retention policy) need to be updated and that they are being followed throughout the organisation.
- ✓ Review the databases, systems, and resources that you have so that you can keep all personal data safe and manage communication preferences.
- ✓ Get your trustees involved – your approach should be agreed at Board level
- ✓ Think carefully about all the relevant information – how many supporters do you have? What's your fundraising strategy? How would you manage going to an 'opt in' system if you chose to?
- ✓ Get help if you need it! You may well need some professional or legal advice to talk you through your situation and any specific issues or questions.
- ✓ Remember – whatever approach you adopt should tie in with your organisation's values. Would you feel comfortable and confident in explaining your approach to your supporters – and the regulators?

PART THREE
FAQS

Can we use both legitimate interest and consent? Or do we have to choose just one and stick with it?

Both are valid conditions to be able to send direct marketing, so you'll need to make sure that whoever you want to send direct marketing to, you are able to satisfy the legal requirements. You might decide that you want to move to consent for all new supporters (opt in), but want to keep relying on the legitimate interests conditions for past donors who haven't opted out (see the example given in the legitimate interest table above). You could then choose to say to those existing donors that you are now seeking their consent for future mailings (which would require a positive action), or you could give them an opportunity to object to future contact (although remember that the legitimate interest condition won't mean you can keep mailing them forever, and cannot be used for some forms of communication such as email marketing to individuals).

There might be a group of supporters who you specifically want to seek consent from, rather than rely on legitimate interest. This will depend on a particular fundraising campaign or the relationship you have with those individuals. That's ok – you can ask for consent from some supporters or for some campaigns without adopting a complete blanket rule either way. But, be sure that you can identify which supporters have consented or not and that you have the systems to administer this properly. If, for example, you are asked by a regulator about how you are communicating with your supporters, would you feel confident that you could provide the relevant information and evidence?

When is consent likely to be most appropriate and least appropriate?

The ICO says that consent is likely to be appropriate 'if you can offer people real choice and control over how you use their data and want to build their trust and engagement.' If you are able to get consent, it is the safest way of processing data provided you have been clear about how and why it is being processed.

However the ICO notes that 'consent is not appropriate when a genuine choice is not available. If consent is a pre-condition of a service, then it is unlikely to be the most appropriate'. If you are unable to offer choice then you must not use consent as a lawful basis.

When is legitimate interest likely to be most appropriate or least inappropriate?

Legitimate interest may be appropriate in situations where it is impractical to ask for consent, or difficult to keep a record of it.

For instance, many individuals may miss out on communications due to simply not having seen your approach for consent. These individuals may still want to communicate with you, but if you have not had a response, you cannot assume consent.

Using legitimate interest as a lawful base forces you to consider whether what you are doing is legitimate and how it affects the rights of individuals. That process may also help you identify risks and improve safeguarding procedures, although you should be thinking about that anyway.

Legitimate interests is not likely to be appropriate if it is difficult to demonstrate the expectations of the individuals, for instance if they have not been given clear information about how their data would be used. It is also probably not appropriate for direct fundraising if your methods are intrusive, since that will make it hard to meet the balancing test. Finally, remember that certain methods of direct marketing (such as emails to addresses owned by individuals) always require consent.

How long can we keep sending direct marketing to supporters? Is there a limit to how long consent lasts?

There is nothing in law, which sets a cut-off point for when you can no longer send direct marketing to individuals – whether you are using consent or legitimate interest. The consent guidance from the ICO says that "it will depend on the context. You should review and refresh consent as appropriate". The Fundraising Regulator says that:

"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?"

Whilst not a rule, the ICO and Fundraising Regulator suggest that a 24-month period for refreshing consent would constitute best practice.

Things to consider include: how often you contact the individual; how intrusive that communication channel is; any factors which would give people a reasonable expectation of a time limit, for example were they donating to a specific time-limited appeal; as well as the relationship between an individual and the cause; and any donor insight or evidence. It's important that you keep a record of decisions you take and the way that you came to those decisions.

If you are relying on the legitimate interest condition, the condition lasts provided you can demonstrate that the individual's expectations would not have changed over time and your interest is not overridden by the individual's rights. However, a regular refresh of your mailing lists will be necessary to ensure you are complying with other requirements of data protection law (including the obligation to keep information accurate and up to date).

Some of this seems quite subjective, people might have different expectations of what's reasonable, how do we decide?

The key thing is for you to be as clear as possible about what future communications the individual will receive at the point of them giving you their data. What will be 'reasonable' will depend on what you told them.

For example, if an individual is donating in support of complete renovation of an old theatre which is likely to take 3 years until it's open and you've only said that that you'll send them regular updates of progress and an invitation to the opening event, then you've created a reasonable expectation of when and why that individual will receive that information from you.

You will need to obtain refreshed consent to keep them on your mailing list once the theatre is open. However, you could originally have created a different reasonable expectation if you were to be clear that you'd also keep them up to date with the programme of performances once the theatre has opened. That's why being clear at the outset is so important.

Also, you can set organisational policies around contact and marketing. It might be that you take a decision not to contact individuals unless you receive some form of positive action or indication from them within 24 months. If you tell people this, and have it clear in your privacy policies, then it's hard to see how it will be reasonable to contact them after the 24 months has passed.

Can we continue to use our 1998 Data Protection Act consents?

If consent was obtained prior to the introduction of GDPR, it may still be able to be used for justifying data processing. However this is only applies if it meets the existing data protection requirements. If not (for example consent boxes

with opt outs were used) then charities will need to ask for GDPR compliant consent, identify a different justification for data collection or cease the current processing of data.

An individual has indicated they wish to have their information removed from our database. What should we do?

Under GDPR, individuals have a 'right to erasure'. This simply means that an individual has the right to have their personal data erased. If a written or a verbal request is made by an individual to have their information removed, charities are required to remove the data within one month of the request. There are some exceptions where removal requests can be refused:

- In order to exercise freedom of expression.
- To comply with a legal obligation.
- If a task is carried out in the public interest or in response to official authority.
- For the processing or defence of legal claims.

There are some people on our database that we aren't sure when they last donated or when they last interacted with us. It hasn't been recorded whether they have given us their consent or not. What should we do?

First of all you should put in the necessary time and resources to update your database. To send direct marketing you need to be sure you are doing it lawfully and fairly. It is not enough simply to comply with the rules; you also need to be able to demonstrate that you comply. This means that you must keep a record of people's communication preferences and when they have been provided. If you are unable to demonstrate that you have ongoing consent, or (for the legitimate interest condition that the information is up-to date) you will not be able to use it for direct marketing.

If you are not sure that you have their consent to send emails, then do not send them an email marketing message – or even an email to ask them to confirm if they are happy to keep hearing from you. You may be breaking the law. You might have considered contacting an individual in these circumstances to be an administrative data cleansing exercise, but if you are making the contact in order to check if the individual is happy to receive direct marketing in the future, the ICO regards that contact as direct marketing in itself.

For postal direct marketing, where you don't have consent, you'll need to undertake a balancing exercise test to see whether you can rely on your legitimate interest. Is it reasonable to write to them at this point? Are you likely to be overriding an individual's rights? Remember the individual's rights come first over and above your legitimate interest in sending direct marketing.

What are the other things that I can be doing to make sure our charity is treating our supporters' data fairly?

If you are writing to people, whether using legitimate interest or you have their consent, remember that peoples' preferences can change over time. It should be easy for people to withdraw their consent or change their communication preferences. So make sure that with communications that you send to them that you're giving them easy and simple ways to change their preferences or to say that they don't want to hear from you in the future. Also, be prepared to be able to answer questions that your supporters have. People are entitled to ask what information you hold about them and why; you got their data from; seek reassurance about how you keep it safe and secure; or ask you to change how you market to them in the future. You must be able and ready to answer these questions for any supporter whose details you hold.

This has all been about the lawful basis for sending direct marketing. What else do I need to know or think about?

Data protection rules go much further than direct marketing and cover all processing of personal data. This guide has focused specifically on direct marketing, as it's the key area that comes up. But if you are undertaking other processing of personal data then make sure you are familiar with the full requirements of the GDPR by reviewing the ICO's guidance.

Are we able to look at information available on public networking sites such as LinkedIn, to find out more about individuals we wish to contact or already are in contact with?

It is common for fundraisers to look at the profiles of relevant individuals of particular interest. Legitimate interest would likely be the most appropriate basis for carrying out processing in this area, but you should carry out a Legitimate Interests Assessment to make sure you meet all of the legitimate interest criteria.

What about 'wealth screening', researching, and profiling supporters?

Processing of an individual's data for these purposes has been an area that's been in particular focus recently as a result of investigations and enforcement action by the ICO leading to some charities receiving fines. The ICO has said that it's not that processing data for these purposes is always unlawful, but the key issue is whether individuals are being sufficiently informed and given the right opportunities to agree or object to their data being used in that way.

For more information and guidance about fundraising and prospect research, take a look at IoF's guidance *'Connecting People to Causes: A Practical Guide to Fundraising Research'*

https://www.institute-of-fundraising.org.uk/library/iof-connecting-people-to-causes/

Data protection FAQs

Does my organisation require a Data Protection Officer (DPO)?

Not all charities will require a DPO. Charities and fundraisers will only require a DPO if they carry out particular types of data processing. You will need a DPO:

- If your organisation's core activities require large-scale, recurring and systematic monitoring of individuals.
- If your organisation's core activities require large-scale processing of special categories of data or data relating to criminal offences and convictions. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

You can employ a DPO even if you do not legally require one. If you do, they must abide by the same standards as other DPOs.

How can I minimise data protection risks at my organisation?

One way to assess risk would be to carry out Data Protection Impact Assessments (DPIA) for your main types of data use. DPIA's are valuable because they get your organisation to think about why you are processing personal data and whether this outweighs the risks to the individual.

A DPIA is mandatory under the GDPR if the processing you carry out involves a high risk individual, but a voluntary DPIA can be useful for

other sorts of processing as well. The ICO states that the assessment must include:

- "A description of the nature, scope, context and purpose of the processing.
- Assessing procedures related to necessity, proportionality and compliance.
- Risk assessments for the individuals
- The identification of ways to mitigate any risks that could affect the vulnerable individuals.'

It is also important to ensure that trustees, staff, and volunteers understand how data protection rules apply to the information they use in their roles. One of the best ways to reduce risk is to make sure those people receive practical training on how to keep that information safe and to recognise when something they want to do with the information might not comply with data protection law.

Training should be supplemented by clear policies that people in the charity can use to understand how they should treat personal data.

Top tips for reviewing GDPR policies:

1. Do your staff understand their GDPR responsibilities? If they are not confident then you need to ensure they receive adequate training.
2. Document all the data you store. You need to be able to justify why you are holding data.
3. Review your consent procedures and ensure they are up to date.
4. Assign a Data Protection Officer to manage compliance risks.

Where else to go for help:

Information Commissioner's Office (ICO)
Guidance on Direct Marketing
https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

ICO
Companies receiving unwanted marketing: PECR
https://ico.org.uk/media/for-organisations/documents/1537/companies-receiving-unwanted-marketing.pdf

ICO
Guide to GDPR
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

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

Privacy Impact Assessment Code of Practice
https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

Fundraising Regulator
Code of Fundraising Practice
https://www.fundraisingregulator.org.uk/code-of-fundraising-practice/code-of-fundraising-practice/

IoF and Fundraising Regulator Spotlight Series

GDPR & Charitable Fundraising: Spotlight on Charitable Trust fundraising
https://www.fundraisingregulator.org.uk/sites/default/files/2018-07/GDPR-briefings-trust.pdf

GDPR & Charitable Fundraising: Spotlight on Legacies
https://www.fundraisingregulator.org.uk/sites/default/files/2018-07/GDPR-briefings-legacies.pdf

GDPR & Charitable Fundraising: Spotlight on Community Fundraising
https://www.fundraisingregulator.org.uk/sites/default/files/2018-07/GDPR-briefings-community.pdf

GDPR & Charitable Fundraising: Spotlight on Corporate Fundraising
https://www.fundraisingregulator.org.uk/sites/default/files/2018-07/GDPR-briefings-corporate.pdf

Institute of Fundraising

GDPR:
THE ESSENTIALS FOR FUNDRAISING ORGANISATIONS

Disclaimer:
This publication is not meant as a substitute for legal advice on particular issues and action should not be taken on the basis of the information in this document alone.

Neither the Institute of Fundraising nor BDB Pitmans LLP make any warranty, representation or guarantee, express or implied, as to the information contained in this guide.

www.institute-of-fundraising.org.uk
020 7840 1000 @IoFtweets

The IoF is a charity registered in England and Wales (No 1079573) and Scotland (No SC038971), and a company limited by guarantee (No 3870883).