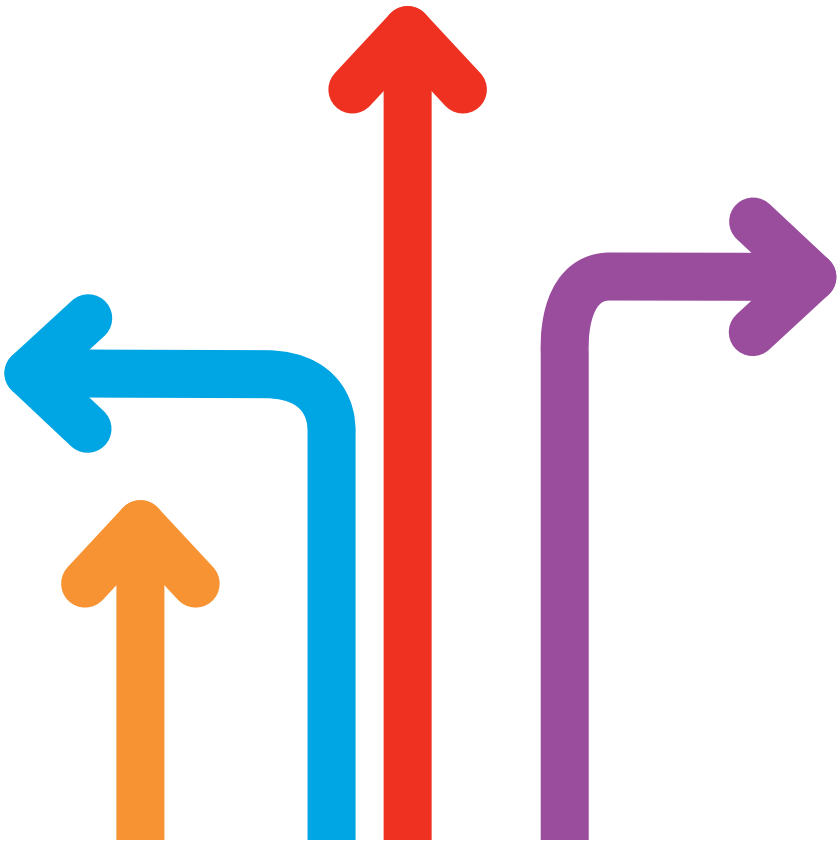
Institute of Fundraising

In partnership with

BIRCHAM DYSON BELL



GDPR:

THE ESSENTIALS FOR FUNDRAISING ORGANISATIONS

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 560 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 Bircham Dyson Bell

Bircham Dyson Bell is an award winning, top 100 UK law firm with offices in London and Cambridge. 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.

https://www.bdb-law.co.uk/

ABOUT THIS GUIDE

On 25 May 2018 the new General Data Protection Regulation (GDPR) will come into effect in the UK. This will replace the current Data Protection Act and introduce new and different requirements for all sectors and organisations. Charities, alongside any private sector organisations, businesses, or public bodies, will have to follow these legal requirements when processing individuals' personal data. So, what's going to be different about the new rules that are coming in? What are the key changes you need to be aware of? How will it impact on how and when you can contact your supporters? Should you go 'opt in' or can you rely on 'opt out' mechanisms? And what are the practical things that you can be doing right now to get ready?

We have put together this short guide to answer those really key questions. We know that all fundraisers and charities want to get this right and want to be sure that they're meeting their legal requirements as well as giving their donors a great experience of supporting that 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

It is also for all types and sizes of organisation. GDPR applies to 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 questions on direct marketing that our members and the wider fundraising community are asking.

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.

Many of the requirements set out in this guide apply already. For more information on your current obligations 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 consent and the use of personal data in fundraising which is available at www.fundraisingregulator.org.uk

A note on what's next

We have written this guide on the basis of current information available. But there is more to come and we expect final guidance on different areas of the GDPR to be published by the ICO over the coming months. We will update this guide when more information is available but do check for latest news!

PART ONE
GETTING TO GRIPS WITH THE BASICS

What is GDPR?

The General Data Protection Regulation is an EU-wide regulation which will become effective in the UK on 25 May 2018. It replaces the existing law we have on data protection (the Data Protection Act 1998) and gives individuals more rights and protection in how their personal data is used by organisations.

But we are leaving the EU – will this apply?

Yes. The ICO have been clear that in May 2018 the requirements of GDPR will 'go live' here in the UK. So get ready for it!

Are the rules the same for everyone – do charities have to comply with the same requirements as businesses?

Charities have to comply with GDPR just as businesses will.

When do we have to be ready?

25 May 2018. That's when GDPR comes into effect. At that point it's expected that you'll be ready and meeting the requirements. That's why we're publishing this guide now so that you have time to think through and implement changes. However, many of the requirements mentioned in this guide already apply under the Data Protection Act so you should ensure you are compliant with existing requirements and start preparing for the GDPR.

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 will be updated to incorporate the relevant requirements of the GDPR.

The Fundraising Regulator can also set standards that go further than the law requires, and in many places it already does. For example, the Code requires charities not to sell supporters' data, and only to share it with another organisation if the individual has given their explicit consent – this goes beyond the legal requirement. So, to meet expected standards of fundraising as well as getting yourself ready for the legal changes, make sure you know what's in the Code of Fundraising Practice.

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 to 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 about promoting products or services. So, if you are a charity and 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 them an email, or calling them on the phone.

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

At a glance: communicating through different channels

Remember, there are some forms of communication, and some types of processing of data, that always require you to have Consent. Under ePrivacy laws you will need consent to be able to send direct marketing by:

- Email;
- 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.

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 – getting ready:

- ✓ Work out who in your organisation is going to be taking 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's anything where your organisation is processing personal data of individuals. So that applies for 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. 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. It's really important that you think all of this through properly before taking a decision which could well have long-term impact for your charity and supporters.

- ✓ A whole organisation approach is necessary with a strategy agreed at Board level following an understanding of your choices and the opportunities or challenges. 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 and unilateral decisions.

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

Ok. We know that this is the big one that people want to know about. It's been the subject of lots and lots of debate and discussion and we know that many fundraisers are scratching their heads not quite sure what changes GDPR brings – what they HAVE to do – compared with ideas on good practice or recommendations. Some large national charities have decided to go all 'opt in'. Others are choosing to remain 'opt out'. We'll try and take you through what you need to know...it is a little tricky so we'll break it down to try and make sense of it.

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 different channels (see the 'At a glance' boxes above for information on where opt in consent is required).

Remember as well that this guide is about '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 is required now. 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 some form of positive '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.

The key thing is that there is some clear action where people have been given really clear information and are able to make a genuine choice to give their consent. Silence or pre-ticked boxes do not count as valid consent.

However, 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 had the opportunity to say 'no' or object to future direct marketing, which is often done through an 'opt out' tick box.

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

Under both the current data protection rules, and the future GDPR, organisations can lawfully send direct marketing by post (or make 'live' calls to people who have not objected or registered with TPS) 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 would not have reasonably expected the information to be used for direct marketing, it would not be legitimate for the organisation to do so.

You should be thinking about 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 interests 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 be useful in helping 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 you charity's legitimate interests in sending the material.

Just like the current 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 balancing assessment to think all this through and to give thought to the individual's rights and expectations.

The examples in the table below gives an illustration of how you could 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 of 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.

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. You will need to think through what is the right thing for you to do, 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 can see case studies of what some charities are doing on the Fundraising Regulator's website https://www.fundraisingregulator.org.uk/wp-content/uploads/2017/02/CaseStudiesFinal.pdf

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 think about 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 do the Regulators recommend?

Both the ICO and Fundraising Regulator say that 'Consent' is the safest basis to rely on for sending direct marketing.

The ICO are clear that Consent is one lawful basis for processing data, but it won't always be the easiest or most appropriate – you should always choose the lawful basis that most closely reflects the nature of your relationship with the individual and the purpose of the processing.

The Fundraising Regulator says that you should only rely on legitimate interests where you can prove that the data was obtained fairly and lawfully, and that you publish your 'balancing exercise' to show how you can justify the condition and be confident that you are not harming the freedoms and rights of individuals.

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 how to come 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.
- ✓ You will also need to review the databases, systems, and resources that you have so that you can keep all personal data safe and manage communication preferences.
- ✓ This is really important for your income, services, and how you go about fulfilling your charitable objectives. Get your trustees involved – your approach should be agreed at Board level.
- ✓ More haste, less speed – yes, you do need to deal with this and make some decisions. But you should take enough time to make sure that you're doing it sensibly and with all the right information to make the right decisions for you (but do remember that GDPR is effective from May 2018!)
- ✓ 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

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

A: 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 send communications to 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).

There might be some groups of supporters who you specifically want to seek consent from rather than rely on legitimate interest depending 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 careful here that you are able to be sure 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?

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

A: 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 draft 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?"

While not a rule, the ICO and Fundraising Regulator suggest that a 24 month period may well be appropriate to renew consent as best practice.

When you are considering how often to renew consent some of the things to consider include: how often you contact the individual; consideration of 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; 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 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).

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

A: 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 that 24 months has passed.

Q: 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?

A: 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.

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

A: 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 on communications that you send 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; where 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.

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

A: 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 doing other processing of personal data then there are issues to think about so make sure you are familiar with the full requirements of the GDPR by reviewing the ICO's guidance.

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

A: 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 on using data in this way, take a look at the guidance from the ICO at https://ico.org.uk/media/about-the-ico/documents/2013426/fundraising-conference-2017-paper.pdf

Q: Ok. So I think I've got the basics now. Is there anything else I should be looking out for?

A: We have written this guidance based on the requirements of GDPR, the draft guidance on consent issued by the ICO in March 2017), and the Fundraising Regulator's guidance 'Personal Information and Fundraising: Consent, Purpose, and Transparency.' It may be that guidance changes or gets updated as it gets nearer to May 2018 – and we expect the ICO draft guidance to become finalised, and possibly complemented by further pieces. As we find out more we'll update this document. But it's worth you also registering for updates from the Fundraising Regulator and ICO so that you'll be up to date with changes as they happen.

Where else to go for help:

Information Commissioner's Office
Guidance on Direct Marketing
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/

Personal Information & Fundraising: Consent, Purpose and Transparency
https://www.fundraisingregulator.org.uk/information-registration-for-fundraisers/guidance/personal-information-fundraising-consent-purpose-transparency/

Institute of Fundraising

GDPR:
THE ESSENTIALS FOR FUNDRAISING ORGANISATIONS

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).