GENERAL DATA PROTECTION REGULATION

A briefing for foundations

INTRODUCTION

The General Data Protection Regulation (GDPR) came into effect on 25 May 2018. It has enhanced the standards of data protection for all organisations handling EU citizens' data, affecting the smallest grant-making trusts to the largest multinational corporations.

The Information Commissioner's Office (ICO) is responsible for the implementation of the principles of the GDPR in the UK. It has published a number of resources including guidance, toolkits and checklists on its website. This should be your first port of call for information. There are resources specifically for charities and for small and medium sized enterprises which will be most applicable to foundations. The ICO has also opened a helpline for small organisations (0303 123 1113 and select option 4).

Having read the ICO's *Guide to the GDPR* and followed its links to European regulation and other guidance, you may still be left with questions about how it applies to your particular circumstances. The ICO's *FAQs for Charities* is a helpful resource which sets out the regulator's response to a number of questions, as well as clarifying what charities can expect, to help them prepare for the GDPR. However, there are still specific questions that arise for foundations.

The aim of this briefing is to answer those questions, to assist in understanding the guidance through examples, and to signpost relevant pieces of guidance and regulation that hold fuller answers. This document is based on the concerns raised by ACF members, as well as some other issues we have spotted. We have engaged with the ICO in producing this document in response to specific concerns.

This guide should only be used in addition to the ICO's own guidance and resources, and does not constitute legal or professional advice. Where necessary, foundations should seek their own advice from the ICO or legal advice.

CONTENTS

The questions in this briefing have been categorised as far as possible under the headings used in the ICO's Guide to the General Data Protection Regulation:

KEY DEFINITIONS

1) What constitutes personal data?

Personal data refers to any information which can be used to identify an individual directly or indirectly. This means any information you hold containing someone's name, address, phone number, National Insurance number, etc. in a way that identifies that individual constitutes personal data. That also includes reports or recordings of conversations in which you refer to a staff member by name or in a way that could identify an individual. Examples would include an email address like jane.doe@abccharity.org.uk, because only one Jane Doe works at ABC Charity, or a comment about the CEO of ABC Charity, because that person can easily be identified indirectly. This means that the personal data you process on staff members at other organisations (e.g. the CEO or your point of contact) could easily be personal data if it identifies them.

For the most part, if information is personal data under the Data Protection Act, it will still be personal data under the GDPR. The difference is that the GDPR expands the definition of personal data to cover new developments in technology where individuals can be identified, such as IP addresses. Pseudonymised data is considered personal data, but it can be a useful way to enhance privacy if the key to decipher the identity of the individuals is kept separately. Sensitive personal data also remains largely the same as under the Data Protection Act. It includes genetic data and biometric data, as well as information on race, ethnicity, sexuality, or religious belief.

For foundations making grants to individuals, some of the information you hold may constitute special categories of data and will require greater consideration when processing. Such data can only be processed for the reasons outlined in Article 9 of the GDPR. If you use sensitive or special categories of data, it is very important to consider these rules and it may be worth taking bespoke legal advice.

But none of this means that you can't process that data; what matters is the *purpose* of processing that data and the lawful basis for doing so.

Article 9

2) Are beneficiary, staff, trustee, and parent company employee data to be treated equally?

Yes, all data relating to a directly or indirectly identifiable individual is personal data and the GDPR applies equally. There will be different reasons for processing each group's data and you will have to determine the lawful bases accordingly, but it all falls under the scope of the GDPR.

ICO guidance on key definitions

3) Which of our activities constitute direct marketing?

Direct marketing refers to materials used to sell a product or service, and importantly, to promote "aims and ideals". This means your newsletter, event invitations, publicity for a new grants programme or funding opportunity, and research publications would all constitute direct marketing if they could be seen to promote your aims and ideals.

Sending direct marketing to an organisation as a whole (e.g. not naming any staff on an envelope or sending to info@abccharity.org.uk) does not fall under the scope of the GDPR, so this is an acceptable way to conduct direct marketing. If you are marketing to individuals, you will need to consider your lawful basis for doing so.

Direct marketing to individuals – even individuals at organisations if they can be identified from the data you hold – must have a lawful basis. Direct marketing to individuals sent by electronic means requires consent under the Privacy and Electronic Communications Regulation (PECR). Therefore, if you are sending newsletters, invitations, or notifications of funding opportunities by email, you'll need to have consent for this. That might mean that during your grants process, you ask whether individuals wish to opt in to such marketing (while letting them know that it will not affect their chances of receiving a grant if they decline). If the direct marketing is sent by non-electronic means, other lawful bases such as legitimate interests may be relevant.

It is really useful to know about the provisions for **corporate subscribers** under PECR when thinking of your organisation's marketing. When contacting a corporate subscriber or an individual working there, the GDPR still applies but you may lawfully be able to send them direct market on the basis of legitimate interests, and not have to rely on consent. A corporate subscriber is a certain type of organisation (generally a corporate body, including many charities), and if their work is directly relevant to the communication being sent, you might have reasonable grounds to rely on legitimate interests to contact them. For example, notifying a fundraiser of a new grants programme, or inviting the chief executive of a housing charity to an event you're hosting on homelessness in the area, would likely fall under this description. The Institute of Fundraising's *Spotlight Series* has some user-friendly information on corporate subscribers.

ICO guidance on key definitions
Articles 2, 4, 9, 10
Recitals 1, 2, 26, 51
Privacy and Electronic Communications Regulation

4) Are we a data controller or a data processor?

A data controller is the person or body which determines the purpose of processing data. A data processor is a person or body which processes the data but does not have any decision making power in how the data is used.

For foundations, you are a data controller when you decide what the data is processed for. This could cover the data you require in applications, the monitoring reports you require from grantees

to demonstrate your impact, or the case studies or photos you use for marketing, for example. A foundation would be a data processor if it only processed the data on behalf of others. Examples of data processors would be MailChimp, Salesforce, your IT provider, or the company that handles your shredding, which all process the data you supply but do not determine the purpose of processing that data.

When collaborating with other foundations, data protection will have to be a consideration. For example, you may contribute to a funding programme with several other funders, and tasks such as processing applications and following up with grantees are divided up between those involved. In this case, responsibilities must be clearly and transparently allocated. That includes things like deciding who is responsible for dealing with subject access requests or reporting a breach to the ICO.

ICO guidance on contracts between controllers and processors
Article 26
Recital 79

5) Do we still have to register and pay a fee to the ICO?

Yes. According to the new three-tier fee structure, charities will only be liable to pay the tier 1 fee of £40, regardless of their size, unless they're otherwise exempt. If you are currently registered and paying the fee, you will not have to pay the new fee until your current registration expires.

ICO: The data protection fee: A guide for controllers

6) Does the GDPR only apply when using platforms like MailChimp and not to our emails?

This is incorrect. Some organisations may come to this conclusion because their direct marketing is likely to be sent by MailChimp and procedures for processing data in this manner must indeed be compliant with the GDPR. However many smaller organisations will use Outlook or other email providers for direct marketing (as defined above), and therefore must ensure these processes are compliant too.

7) How does the GDPR apply retrospectively?

All data processed will have to have a GDPR-compliant lawful basis for doing so. Foundations will have to look at what the lawful basis is for processing pieces of data and whether it still applies. For example, if you hold data that was obtained in relation to a grant that is ongoing, the lawful basis likely still applies. If that grant was a one-off several years ago, you should consider why you still hold that data and whether there is a lawful basis for continuing to hold it. If not, it should be erased or anonymised as appropriate.

If you process data based on someone's consent, for example to receive newsletter updates, you should look at how that consent was obtained. If it was obtained in compliance with the GDPR's high standards and within a reasonable timeframe, it is still acceptable to process the data. If not, you will have to obtain new consent in a way that complies with the GDPR. This might be writing to someone by post to ask if you can email them, if you don't already have consent to contact them by email. You are permitted to change your lawful bases, but you still need to assess thoroughly the grounds for doing so. For example if you previously relied on consent to publicise your funding opportunities, you may review its lawful basis and decide that you can satisfy the criteria of legitimate interests, but you will need to show that you have thought this through.

If the only reason you retain data is for archiving purposes and you don't actively process the data, this may be covered by provisions for archiving. See the question on archives later in this briefing.

8) Does GDPR apply outside of the UK?

The GDPR applies to all organisations handling EU citizens' data, whether the organisation itself is based in the EU or not.

There are provisions around transferring data outside the EU; basically, you must be confident that the organisation you are sharing with is aware of your data protection requirements and responsibilities and has adequate measures in place to meet those, which you could then demonstrate if requested. If you are dealing with giant American companies – Google, Microsoft, etc. – they will likely have in their terms and conditions that they meet European data protection standards, as they have to in order to operate in the EU.

For foundations whose direct or indirect beneficiaries are citizens outside the EU, it is the fact that you are based in the EU and that you have to comply with the GDPR that is important. Therefore personal data, collected for example for case studies in your marketing materials, must meet the GDPR's requirements.

Articles 46, 49
Recitals 108, 109, 110, 113, 114

9) What about data we collect and pass on to event venues about access and dietary requirements?

It is likely that you'll be able to find a lawful basis for processing such data, for example legitimate interests or to comply with disability legislation, and what's more, individuals are likely to understand why processing this data is necessary without complaint. As such, the risks are low. But this is something to consider in your data retention schedule to demonstrate how long you will hold this data and if/when it will be erased or anonymised.

ICO guidance on lawful bases for processing

10) Are bank details sensitive data?

Bank details are personal data if they belong to an individual, but not sensitive data. It is likely that you will have a lawful basis for processing individuals' bank details for the purposes of paying staff or making grants.

ICO guidance on lawful bases for processing
ICO guidance on key definitions

LAWFUL BASES FOR PROCESSING DATA

11) Which lawful basis best covers our grant-making activity?

There are six lawful bases for processing data; each one is equally valid but they all carry different implications. They are discussed in turn below.

ICO guidance on lawful bases for processing
ICO: Lawful basis interactive tool
Articles 6-10
Recitals 38, 40-50, 59

a) Consent of the data subject

You can legally process data if you have the consent of the data subject. Under the GDPR, there can be no vague explanations, blanket consent, or small print hidden among other terms and conditions. Consent must be freely given, specific, informed and unambiguous, including why and how the data will be processed and by whom. It must also be granular, so if for example you are obtaining consent to send a variety of marketing materials, you must say what they are (e.g. event invitations, newsletters, etc.) and by which channels they will be sent. Consent must be as easy to withdraw as it is to give. And importantly, there must be a record of consent being given. In practice, this suggests most organisations will need to adopt an 'opt-in' approach to seeking consent.

As far as documentation is concerned, obtaining consent to the GDPR's standard would be sound proof of your rationale for processing data. If you have compliant consent, there can be no denying that the individual knew how and why their data was being processed, should the ICO ever ask for this. But if relying on consent, it is vital that it meets the GDPR's high standards. If it proves difficult to obtain consent, it may not be the most appropriate lawful basis.

Some have raised concerns that the power imbalance between the foundation and the grantee is such that individuals may feel compelled to give consent – in which case the consent is not freely given and therefore not compliant. To avoid this, it is worth letting individuals know that not giving

consent does not affect the grant-making process; consent cannot be a pre-condition for something else, so individuals should not feel pressured to, for example, sign up to your newsletter just because they perceive it to be necessary to receive a grant.

ICO guidance on consent

b) Necessary for the performance of, or to enter into, a contract with the data subject

The ICO is currently working on further guidance on contracts as a condition for processing data. Its interpretation of a contract here is in line with contract law. That means that to use this lawful basis, the data controller would have to be satisfied that the definition under contract law is being met.

Some foundations have asked whether their grants could be considered contracts and therefore this lawful basis used to process data. This will depend on whether your foundation is satisfied that the grant meets the definition of a contract under contract law. If your grant agreement doesn't meet this definition, this isn't an appropriate lawful basis.

ICO guidance on contracts

c) Necessary for compliance with a legal obligation

This lawful basis is likely to be the grounds for processing data on staff, volunteers, and trustees. You may also have other legal obligations; for example, if you are affected by the Common Reporting Standard you are required to hold data on grantees' tax status for up to six years, or if you have been involved in a regulatory case you may also be required to process data relating to that.

ICO guidance on legal obligation

d) Necessary to protect the vital interests of a data subject or another person

This relates to situations in which the organisation processes data in order to provide directly life-saving or urgent treatment, for example needing to know a patient's blood type when the patient is unconscious in order to undertake a blood transfusion. In general, the ICO is unlikely to consider that this lawful basis is applicable to foundations as they are somewhat removed from this kind of direct and immediate data processing.

ICO guidance on vital interests

e) Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

There may be cases where this lawful basis is appropriate, but the ICO is likely to require strong justification for this and supporting evidence that the balance of public interest lies in favour of the data being processed. Although there have been suggestions that charities' requirement to exist for the public benefit might make this lawful basis applicable, the ICO suggests it would be difficult to argue that this would cover all of a charity's activity as far as data protection is concerned.

ICO guidance on tasks in the public interest

f) Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

Using legitimate interests as a lawful basis involves a balancing exercise between your interests and the rights of the individual. It is the most flexible of the lawful bases, but standards must still be met to ensure that the processing is in keeping with the GDPR's principles.

The ICO has a three-part test to establish whether it's an appropriate basis. It includes: identifying the interest; showing that processing is necessary; and balancing the interest against the rights of the individual, which now includes asking whether the individual could reasonably expect the processing. The ICO also has detailed guidance on when legitimate interests are an appropriate basis with a checklist to guide you through decision-making. When you have decided that this is an appropriate lawful basis, you should document your rationale and make it available in your privacy notice.

It seems likely that most foundation activity would be lawful on this basis. For example, if you process individuals' data to evaluate the impact of your grant, you could say that this helps you achieve your charitable objectives, that there is no other way to measure impact, and that the individual could reasonably expect you to do this as you told them. Another example may be sharing your recent research on the benefits of children taking part in sport with individuals at local youth charities; you might say it is in the wider societal interests, that there's no more intrusive way to get the research to them, and that the individuals will find the research relevant and interesting in their line of work.

ICO guidance on legitimate interests

12) Do we need consent to continue means-testing for our welfare assistance grants?

As ever, you will need a lawful basis if processing individuals' data. This may take the form of consent or there may be other lawful bases as described above. For example, where an individual may be the prospective beneficiary of welfare grant but unable to provide consent for reasons of health, age, capacity or other.

If your means-testing involves working with a third party, either as a joint controller or a data processor, you should ensure you have discussed data protection requirements with them and reached an agreement that is compliant.

If you are concerned about processing special categories of data, it may be best to seek bespoke legal advice.

ICO guidance on special categories of data
ICO guidance on criminal offence data

INDIVIDUAL RIGHTS

13) What do we do in response to a subject access request?

Under the GDPR, individuals will have rights to access and amend their data. An individual asking to see a copy of the data you hold on them is called a subject access request (SAR). This is already permissible under the current Data Protection Act and organisations are able to charge £10 for such requests. The GDPR abolishes the charge, so organisations will be expected to provide the requested information for free unless the request is "manifestly unfounded or excessive, particularly if it is repetitive". Organisations have at most one month to respond, which is shorter than the 40-day period under the DPA.

Individuals can request to see all data held on them that is held in a relevant filing system, e.g. in folders, on a database, in records of conversations, or in emails about them, etc. so it is vital to know where you keep your data and what the procedure would be for collating it.

There are exemptions to the data you have to provide. For instance, if an individual who has requested access to their data has a diagnosed mental health disorder, and providing them the data would cause them further harm or distress, this would qualify for exemption. See Article 23 of the GDPR for a list of restrictions and exemptions, and look out for the Data Protection Bill for more information on exemptions in the UK.

There are exemptions to the data you have to provide. For instance, if an individual's data is inextricably linked to the personal data of another individual, this may be grounds for exemption.

Embarrassment is not a reason for exemption. For example, if you have recorded on your grants management software that Jane of ABC Charity is a weak leader, Jane Doe would have the right to access such data. If Jane Doe feels this data has been unlawfully processed, she can request that it is erased.

ICO guidance on subject access requests
ICO guidance on employment and references
Article 12, 15, 21, 23
Recital 63

14) Will our existing terms and conditions need to be updated?

If your terms and conditions don't already meet the GDPR's standards, they will need to be updated. The changes you need to make will depend on the kinds of activity you undertake, the audience you are working with, and the lawful bases you are using (e.g. to obtain consent it will need to be granular). Data protection should no longer just be bundled into your existing terms and conditions; your privacy policy or notice will need to be drawn to attention as described above.

15) Is it acceptable to keep a record of contact with an individual whose data was obtained from ABC Charity but who now works with XYZ Charity?

Although this is not necessarily common practice, it could be a tricky area to navigate when it does occur and may require some sensitive handling. Such a case may arise if, for instance, a foundation made a grant to ABC Charity and during the experience found the CEO to be dishonest or incompetent. That CEO now has a new position with XYZ Charity, and the foundation feels it risky to consider working with that individual again.

If the case in question resulted in a legal case, such as a regulator's inquiry or a criminal investigation, the foundation may have a legal requirement to retain such information – and so a lawful basis to process it. However if the case in question is based on opinion, this may not be justification enough to keep the individual's data. For the ICO to see this use of data as justified there would have to be concrete evidence – such as a clear example of wrongdoing or criminal activity – to base the opinion on. Having a bad experience with someone or suspecting them of wrongdoing is not likely to be enough to satisfy the ICO that processing their data for such purposes is acceptable. This is similar to the ICO's current approach under the Data Protection Act and is unlikely to change under the GDPR.

ICO guidance on the right to be informed
ICO guidance on the right to erasure

ACCOUNTABILITY AND GOVERNANCE

16) Is it sufficient to put our privacy notice on our website?

Not generally. The GDPR places emphasis on the rights of individuals and the principles of transparency and accountability. That means the individual has to be aware of their rights and how to exercise them, and they must be fully informed of how and why you're processing their data. This should be communicated in a privacy notice or privacy policy that you actively draw to their attention. There is still scope to take a 'layered' approach, so for example having a shorter version on forms which clearly directs individuals to the full version is acceptable.

How this looks in practice is up to you; you will need to consider who you are talking to and how best to communicate with them at the earliest opportunity. For example, the privacy policy of an organisation that makes grants to registered charities in the UK will be very different to that of one making grants to individuals whose first language is not English. If possible, ask someone skilled in communications to draft or review your privacy policy. Simply publishing a notice passively on your

website is unlikely to be sufficient; the expectation will be that you have actively tried to provide or signpost this information to relevant parties.

17) What should we include in our privacy notice?

The ICO has a checklist to ensure you cover the basics within your privacy notice. What it looks like in practice will vary greatly depending on the intended reader and your reasons for processing their data. The essentials include things like your details (as the data controller), the categories of data you'll process, your reasons for doing so, and any third parties you'll share with. You'll also need to include your data retention schedule to show individuals how long you will keep their data and when it will be erased or anonymised, and if relying on consent when that will be refreshed. If relying on legitimate interests for any processing, you'll need to lay out what those interests are and how you reached that decision. And explicit under the GDPR, you'll need to make it clear what rights the individual has and how they can exercise them.

ICO guidance on privacy notices
ICO guidance on the right to be informed (including checklist)

18) Do we need to appoint a Data Protection Officer?

Only certain types of organisations will need to appoint a Data Protection Officer (DPO): public authorities, those undertaking large scale systematic monitoring, or those processing sensitive data on a large scale as a core activity.

It is highly unlikely that a foundation would need to appoint a Data Protection Officer on the first two conditions.

Foundations processing sensitive data – for example, making grants to vulnerable individuals or faith-based charities – are unlikely to be processing the data as a 'core activity' (their core activity being grant-making) as described in the third condition. You may have knowledge of, for example, your donors' or beneficiaries' faith, but it would be up to your foundation to interpret whether you are processing that data as a *core* activity and whether you would be able to carry out your activities without the need to process this special category of data.

While it may be helpful to identify who within your organisation is responsible for ensuring compliance with the regulation, it is recommended that they are not referred to as a Data Protection Officer. The DPO is a specific legal role with particular duties and obligations under the GDPR – where possible, it is a term best avoided. Instead, you might refer to the person responsible as your data compliance manager or data protection lead.

ICO guidance on data protection officers
Article 37, 38, 39
Recital 97

19) What is a reasonable timeframe to hold data?

This will entirely depend on how long it is necessary to hold the data and how long the lawful basis for doing so is valid. For example, if you award a grant for three years, you are likely to be able to find a lawful basis for processing data for at least those three years. You shouldn't have to erase data that is still being lawfully used.

A good way of handling timeframes is to draw up a data retention schedule. This will set out what personal data you hold, the purpose of processing it, and for how long you will keep it. It will also document if you will require refreshed consent or will erase data at a particular point. When you have data retention schedule, you can let individuals know through your privacy notice.

If you are relying on legitimate interests or consent for direct marketing, they must reflect what the individual can reasonably expect – but this will vary depending on the activity. It is up to you to decide in your context what is reasonable. For example, if sending direct marketing to individuals based on their consent, asking questions about the volume of your marketing, the frequency, and the purpose might help you decide.

ICO guidance on documentation

20) What does the ICO want to see in terms of demonstrating compliance?

The ICO wants to see that organisations have a good understanding of the data they process, and that the principles of the GDPR are being upheld in a way that is relevant, justified and employs common sense. This means showing that you are upholding Article 30 and the accountability principle.

In practical terms, this might mean keeping written records of things like: staff training on data protection, the thought process behind using certain lawful bases, declarations of consent, a data retention schedule, minutes from discussions of data protection, etc. The ICO has a documentation template that might help you document the data you process and the reasons for doing so.

In the unlikely event that a complaint was made against your foundation, these documents would provide evidence of your intention to comply with GDPR requirements; it would still be for the ICO to assess whether they were satisfactory.

ICO guidance on documentation
ICO documentation template
Article 30
Recital 82

21) How can we ensure our data processors are complying with the GDPR when we only deal with huge company tools like Dropbox and Google?

It will be advisable to update contracts with third party IT suppliers to reflect new GDPR requirements. However in practical terms it would be unreasonable if the ICO expected small organisations to negotiate contracts with global companies such as Microsoft and Google. These companies will have to be compliant with the GDPR in order to operate in the EU and process EU citizens' data, so it is reasonable to assume their legal teams will update their terms of service accordingly. If you are unsure, you might want to check whether these organisations are registered with the Privacy Shield (if based in the USA) or if the country in which they are based has been found to have adequate data protection arrangements by EU.

ICO guidance on contracts
Articles 28-36
Recitals 81-83
EU adequacy decisions

DATA BREACHES

22) Are we responsible for those we fund being compliant?

Data controllers and data processors are responsible for their own processing. In this sense, your grantees are ultimately responsible for their own compliance with the GDPR.

Conversations have arisen as to how much foundations should be supporting their grantees in implementing the GDPR. Some are considering making it a term of the grant that organisations are compliant. Others are considering capacity building or other ways in which they can help grantees implement the GDPR, especially those with limited staff numbers who process relatively high levels of data. Many foundations are finding that preparing for the GDPR has led to further reflection on their relationship with grantees and what information they are asking grantees to provide them.

ICO guidance on accountability and governance

23) Would we be liable if someone we funded or worked with went on to experience a data breach?

If you are able to demonstrate to the ICO that you had made satisfactory efforts to be compliant, it is very unlikely that you would be liable, although your liability will depend on whether you are a data controller, data processor, or neither in any given case.

For example, if a charity you fund suffers a data breach in an activity unrelated to your grant and not using data you have provided them, there is unlikely to be anything you are liable for. If that charity is using data which you have provided it in order to carry out a piece of work for you, and then suffers a data breach, you are the data controller (as you determine what is done with the data) and are ultimately liable. If a body is doing work on behalf of your foundation in the capacity of a data processor, for example liaising with tenants in your properties, the foundation should have an agreement in place which covers GDPR compliance.

ICO guidance on accountability and governance

FOUNDATION PRACTICE

24) What do we do about children's data we process?

The GDPR enhances standards of protection for children's personal data. If you are relying on consent, the GDPR states that children under 16 cannot give consent themselves, and in the UK the Data Protection Bill is likely to lower that age to 13. This means that those with parental responsibility for the child must give consent on their behalf.

The ICO has information specifically regarding the processing of children's data. The principles of lawfulness, fairness, and transparency still apply, but must be interpreted with the child's level of understanding in mind. If you are offering services directly to children, for example grants that go straight to an individual child, it is essential that they understand why and how their personal data will be used. This means ensuring that the language used can be understood easily from a child's perspective.

If you are concerned about processing any special categories of data, it may be advisable to seek bespoke legal advice.

ICO guidance on children's data

25) Will this restrict our ability to collaborate with other foundations?

In short, no; that is not the intention of the regulation. But it is vital to consider how data is processed when collaborating and what the lawful basis is for doing so.

For example, you may contribute to a funding programme with several other funders, and tasks such as processing applications and following up with grantees are divided up between those involved. In this case, responsibilities must be clearly and transparently allocated. That includes things like deciding who is responsible for dealing with subject access requests or reporting a breach to the ICO.

Other ways in which foundations collaborate, such as passing on references or recommendations about grantees or potential grantees, will also have to consider how data is used. As with all processing, there will need to be a lawful basis for doing so. If you are sharing personal data with third parties, for example by passing on recommendations or by connecting individuals with one another, they should know you are doing this and there must be a lawful basis. For example, if you are offering a formal written recommendation to another foundation about a charity you've worked with and you're naming its staff or trustees, this could be in your legitimate interests and the third party's having weighed your interests against the rights and freedoms of the individual. See below for more information on references and what the public can expect to see.

ICO guidance on contracts between controllers and processors
Article 26
Recital 79

26) Can we still connect our grantees with one another?

It is likely that there'll be a lawful basis for this, if there is a good reason for doing so. But to be transparent it is worth telling grantees that this is one way that you may use their data and perhaps thinking of getting their consent. Remember that it is personal data which is subject to the GDPR, so connecting two organisations – using their organisational contact details – would not fall under the scope of this regulation. Therefore using generic email addresses (like info@charity.org.uk) to make the initial introduction may be one way to do this.

ICO guidance on lawful bases for processing
Articles 6-10
Recitals 38, 40-50, 59

27) Can we still reach out to individuals and organisations that aren't our grantees but are in areas of deprivation or with low levels of applications to us?

Yes, though you should be clear what the lawful basis is for doing this if using personal data (as opposed to organisational contact information). See above for information on direct marketing.

28) Can we continue to hold archives?

The GDPR applies to the data of living people, so historical records of the deceased are not subject to the GDPR. There are provisions that allow data to be processed solely for the purposes of archiving in the public interest, so keeping archives is permissible.

However if data held in archives is then to be actively processed, for example to get in touch with former scholarship holders to invite them to an event, the data must be processed in accordance with a justifiable lawful basis.

ICO guidance on principles
ICO guidance on exemptions
The National Archives

29) What does the GDPR mean for our ability to share research?

Foundations may wish to share research conducted in the field of their funding priorities, or they may share reports on their own programmes or learning that they feel would inform fellow foundations. There are several considerations when thinking about sharing such research

The first consideration is to see if the GDPR is relevant. Sharing your foundations' research with another foundation or organisation falls outside the scope of the GDPR as it is considered a business to business activity. Identify where, if at all, there is personal data involved. If there are individuals identified within the research, you will need to ensure that their data is being processed in compliance with the GDPR, for example you have obtained their consent to include them as a case study, or the data has been appropriately anonymised or pseudonymised. If there is personal data involved because you are sending the research to individuals, the next consideration is whether the research could be classed as direct marketing.

Direct marketing refers to materials used to sell a product or service, and importantly, to promote "aims and ideals". If the research could be considered direct marketing, you must then consider your lawful basis for sending it to an individual.

The individual may be part of an organisation that meets the definition of a corporate subscriber under PECR; that might be someone within the recipient organisation whose job is directly relevant to the marketing, for example notifying an individual whose role involves raising funds of a new

funding opportunity. To send direct marketing to this type of contact, you may rely on legitimate interests as an appropriate lawful basis.

Where this interpretation doesn't apply, the next consideration is *how* you are sharing it. If the individual is not a corporate subscriber and you send it by post, you can also rely on legitimate interests in these circumstances. If the individual is not part of a corporate subscriber and you send it by email, you must have obtained their consent to the standards of the GDPR. See the responses earlier in this briefing which have more detail on the lawful bases.

If the research could not be considered direct marketing, you may rely on legitimate interests to share it with individuals, though as always a legitimate interests assessment must be done to ensure it does not override the rights, interests and freedoms of the individual.

When sharing research and publications with journalists, the same considerations apply. This might mean reviewing your press contacts and being more selective when sharing your work. But you are likely to be able to find a suitable lawful basis for sharing research with those who are truly interested.

30) Is our grants management system suitable for the requirements of the GDPR?

This is something that you will determine when conducting a 'data audit' – a review of the what, where, who, how and why of your data. You may rely on your grants management system if an individual submits a subject access request and you need to be able to pull a report with the data you hold on them. It is worth checking that you can record things like consent or requests to erase data either on your existing grants management system or another appropriate system.

31) Will our grantees be compliant when collecting data to meet our monitoring and reporting requirements?

This is a conversation to have internally and with your grantees; you may want to think about what you're asking for, whether you have a valid reason for doing so, whether all the data is necessary for your purposes, and whether you are potentially putting grantees in difficult positions. Are you asking grantees for more information about individuals than you need? Would it be just as useful in an anonymised or pseudonymised format? These questions might emerge when you conduct a data audit.

ICO guidance on contracts between controllers and processors
Article 26
Recital 79

32) What do we do about data we collect from a third party for our grant-making?

Some foundations, especially those making grants to individuals in difficult circumstances, may act on referrals or offer grants to those whose data has been collected by a third party, for example another charity like Citizens Advice or a support worker.

The principles of the GDPR still apply to situations like this, whereby the individual must know who is processing their data and why, and give their consent if necessary. This means working with the third party to ensure that the individuals in question know and understand your privacy policy and purposes for processing their data. If the third party is responsible for obtaining consent on which you rely for lawful processing, you must be sure that the consent meets the GDPR's standards.

ICO guidance on the right to be informed
ICO guidance on consent

FURTHER SUPPORT

The ICO

The ICO regulates thousands of organisations in the UK in a wide variety of industries, and is responsible for overseeing the implementation of the *principles* of the GDPR. This means that the ICO is unlikely to produce any prescriptive templates or guidance for very specific types of organisations.

However, it is constantly updating the resources that are available, especially those aimed at small and medium-sized enterprises, which are also relevant to most charities. There will also be further updates to the ICO's resources as the final contents of the Data Protection Act 2018 take effect.

- ICO: For organisations
- ICO: Guide to the General Data Protection Regulation (GDPR)
- EU: General Data Protection Regulation
- ICO: GDPR recitals and articles
- ICO: GDPR FAQs for charities
- ICO helpline for small organisations: 0303 123 1113 and select option 4
- You can also contact the ICO by email here

For foundations

The first port of call should always be the ICO's resources and the European regulation from which it derives. However, other organisations have tailored interpretations that may be of use to foundations and the wider charity sector:

ACF is hosting a number of events in the coming months with a focus on the GDPR. They include the Professional Development Programme, webinars, and various network meetings. Visit the events page of our website for more information (you may need to log in to access the full listings).

For charities

Other charity sector bodies have produced guidance and support for different constituencies which may be a helpful tool to aid understanding of the GDPR:

- NCVO
- Fundraising Regulator
- Institute of Fundraising
- CFG
- NICVA

DISCLAIMER

Please note that although ACF has tried to ensure the information is correct, we do not guarantee the accuracy of these pages and any person using information contained in them does so entirely at their own risk. See our website for more information. If you have any doubts about your duties and responsibilities under the GDPR, please refer to the ICO's guidance, seek professional advice, or contact the ICO.

Version 2 updates

- Amendments made to integrate new ICO guidance and update responses
- Two new questions added
- Broken links removed
- Additional resources included