Lawful Data

a guide for small and new UK charities

to help you process data lawfully

Summary

The Data Protection Act 2018 requires that you process data about people lawfully. That places a set of responsibilities on you, and you need to be able to show that you've met them.

In our previous guide, we helped small charities identify the data they need to fulfil their mission. This guide helps you take the next step, focusing on establishing the *lawful basis for processing* the data you need.

The accompanying workbook to this guide provides a template for you to write down your responses. You'll need to keep this completed workbook as part of your compliance records.

The Information Commissioner's Office (ICO) is the official source for guidance, and they have a lot that's detailed and helpful. We'll link to particular resources through this guide.

Disclaimer: This guide and the accompanying workbooks do not constitute legal advice and are not a substitute for your duty to meet your own data protection obligations. These resources are designed as a starting point to assist small and new UK charities in thinking about their legal obligations and practical data needs and are used at your own risk. You should seek advice from a lawyer or data protection professional for further assistance.

Introduction

You can't just do what you want with the data you have. If it identifies individual people (and a lot of your data will) then you will be subject to the Data Protection Act 2018. There's also the Privacy and Electronic Communications Regulations 2003 (PECR), which govern electronic marketing (which includes charities sending information to people and cookies on websites).

This is the second in a three-part resource to help small and new charities think about how best to use their data to fulfil their missions. If you've not already done so, you'll need to map out the data you have (or need) first—that was the first part of the guide.

This guide is a general introduction to the regulations, and some resources to help you with your own compliance. It helps you think through what lawful basis for processing you are relying on to process the data you use. If you don't have a documented basis for processing, you are processing data unlawfully.

None of this is legal advice. There's a lot of guidance on the ICO website which you should look at, and if you're in any doubt you may need to speak to a lawyer or data protection specialist about your particular circumstances.

Overview of the Regulations

The Data Protection Act 2018 sets the framework for data protection. The act implements the UK General Data Protection Regulation (UK GDPR) and sets out the key principles, rights, and obligations for the processing of data in the UK. These are the principal laws you'll almost certainly need to comply with. The law applies to any 'processing of personal data', so if you have names of supporters, beneficiaries, volunteers, staff members, or trustees and do anything with them, you'll need to comply.

Some jargon: a **Data Controller** decides how and why to collect data; a **Data Processor** may or may not be a separate organisation that processes it on the instruction of the Controller. Your charity is highly likely to be a Data Controller. The obligations on Controllers and Processors are different. The ICO is the regulator for all this and has some useful resources.

There's no checklist—it's a 'flexible, risk-based approach'—the price of flexibility is that you have to think about and justify what you do. Your thinking should revolve around the seven key principles set out in the UK GDPR. In general terms, these are:

- **Lawfulness, fairness and transparency**: you have a 'lawful basis' for data collection. You also need to be clear, open, and honest about who you are, why you are collecting personal data, and how you will use it. Helping you establish the lawful basis for your processing is the focus of this guide.
- **Purpose limitation**: understand and say why you're collecting data, have a legitimate reason, and don't do something other than what you said.
- **Data minimisation**: only collect what you need for your stated purposes, no more and no less.
- **Accuracy**: keep it up to date, and correct errors.
- **Storage limitation**: don't keep it longer than you need to.
- **Integrity and confidentiality** (security): keep it safely. We'll say more about this in the final part of this three-part guide.
- **Accountability**: be able to demonstrate the above—in other words, write down your decisions and rationale. Make sure that everyone in your organisation, at every level, takes responsibility for data protection.

You'll probably have several different categories of data, and you'll need to think about them separately. You may want to collect different information from donors, volunteers, or beneficiaries for different purposes, so you'll need to think about them separately.

The GDPR also gives rights to individuals over their data, which means you may to have to do something if asked. For example, people have a right to access their data, so you need to provide it if they ask, unless certain restrictions apply. There are rights for individuals to be informed, to have their data corrected or erased, to restrict or object to the processing of the data, and to data portability. There are also rights relating to profiling and automated decision making—although small charities are unlikely to be doing this. You should make sure you are familiar with these rights which are set out in the ICO's Guide to the GDPR.

This can all feel quite daunting but the guidance from the ICO is helpful:

- Guidance for small organisations: https://ico.org.uk/for-organisations/sme-web-hub/
- Fundraising and data protection: https://ico.org.uk/for-organisations/fundraising-and-data-protection/

You probably need to register with the ICO and pay an annual fee (£40-£60): https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/

As well as GDPR, you may also need to consider PECR if you wish to send electronic marketing messages (by phone, fax, email, or text message), use cookies on your website, or provide electronic communication services to the public. There's some crossover with GDPR and the fundraising guidance. If you're planning to send out electronic fundraising campaigns you'll need opt-in consent from the recipients, and you'll need to keep records of it. You'll also need the ubiquitous cookie consent on your website. There's more to it than that but the details are outside the scope of this guide. The ICO guidance starts at https://ico.org.uk/for-organisations/guide-to-pecr/.

Our experience and impression of the ICO is that it wants to help you get it right, rather than just clamp down if you get it wrong. They have a helpline you can contact where you can get advice (details at https://ico.org.uk/for-organisations/sme-web-hub/contact-us-sme/). There's also some pretty good guidance from NCVO.

Establishing Your Lawful Basis for Processing

In Part One, you completed a map of the data you have or need about people. You also need to establish the lawful basis for processing it. If you can't establish a lawful basis, you shouldn't process it and will need to dispose of it.

It's likely that different types of data will have different lawful bases for processing.

For example, as you're a charity, you have trustees, and you have their names, addresses, and other information that's required by The Charity Commission. Names and addresses are on The Charity Commission's website.

You have a *legal obligation* to collect this information—that's your lawful basis. But you don't have a lawful basis to process their CV because The Charity Commission doesn't require it. You may judge that you do have a *legitimate interest* in doing so—you need to recruit Trustees, you need a balanced board, you need to make sure you're using all the skills and experiences of your board, and so on. After weighing these organisational interests against the interests of the Trustee and any impacts of your processing, you think about whether there are alternative ways of achieving your interests. You conclude that processing their CV for these reasons is legitimate. That doesn't mean you can do anything with the CV once you have it—putting their CV on your website is less likely to be justified.

There are six valid lawful bases for processing personal data:

(a) **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) **Vital interests**: the processing is necessary to protect someone's life.

(e) **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests (this cannot apply if you are a public authority processing data to perform your official tasks).

Many charities will find that they are most likely to rely on consent or legitimate interests for most of their processing. Some will fall under legal obligation, as in the example above. None of the lawful bases are better than any of the others. The ICO has an interactive tool that can help you decide which apply (in some cases, more than one will apply).

The vital interests basis is quite limited—really only for life-and-death situations. The public task basis is primarily for public authorities: it's unlikely to cover your services provided for or on behalf of a public authority. If you use contracts with beneficiaries, that may be a lawful basis for the data you process in order to carry out that contract but most charities probably won't do so. A contract with a funder to provide a service isn't relevant—the contract has to be with the data subject.

Legitimate Interest

It's tempting to see legitimate interests as a handy catch-all, "Well, we need it so we have a legitimate interest". This is incorrect. It is the most flexible basis, but you are taking on extra responsibility for considering and protecting people's rights and interests.

To rely on legitimate interests, you have to carry out a three-part test:

1. identify a legitimate interest
2. show that the processing is necessary to achieve it
3. balance it against the individual's interests, rights, and freedoms

The ICO refers to this as a Legitimate Interests Assessment (LIA).

The example above of the Trustee CV shows this kind of judgement process. A legitimate interest could be your organisation's interests, or the interests of another organisation or person. The interest itself could be a commercial one, or it might relate to an individual or to society as a whole.

If an individual would not reasonably expect you to use their data as you propose, or if it would cause them an unjustifiable harm, then their interests may override yours. Your organisation's interests may outweigh the individual's interests, but this must be clearly justified.

There is more detailed information on applying the test and conducting an LIA in the ICO guide.

Consent

Consent may seem easier: "check this box—our T&Cs are here". But consent means 'offering individuals real choice and control' and shouldn't generally be a precondition of providing a service.

If you want to rely on consent:

- it needs to be the most appropriate basis
- it needs to be freely given
- individuals should opt in, not opt out
- requests should be specific, clear, and concise
- you need to keep good records of that consent
- you need to provide the data subject with information about your processing and their rights

They can withdraw consent whenever they like, it should be easy for them to do so, and they should be aware that they can do so. You will need to review consents from time-to-time to ensure that nothing has changed.

Suggestions

The lawful basis for holding and processing data about t**rustees** you are required to collect for legal reasons (The Charity Commission, Companies House, etc.) is most likely to be *legal obligation*. The lawful basis for other trustee data is more likely to be *legitimate Interest*, possibly *consent*, or conceivably *contract*.

The lawful basis for holding and processing data about **staff members** (and possibly volunteers) is likely to be a combination of *contract* and *legitimate interests*.

The lawful basis for holding and processing data about **donors** and **supporters** is likely to be *consent* or *legitimate interests*. You will need to judge which is more appropriate.

Data about **beneficiaries** is likely to be covered by *legitimate interests* or *consent*, or conceivably *contract*.

Especially Sensitive Data

Some data falls into special categories and needs to be handled more carefully. Special category data under the UK GDPR is:

- personal data revealing racial or ethnic origin
- personal data revealing political opinions
- personal data revealing religious or philosophical beliefs
- personal data revealing trade union membership
- genetic data
- biometric data (where used for identification purposes)
- data concerning health
- data concerning a person's sex life
- data concerning a person's sexual orientation

If you are processing any of these types of data, you need to meet additional conditions, so check the guidance. Fortunately, being a not-for-profit body is

one of the justifications for this. You also need to decide whether any of your processing is 'high risk', and you may need to complete a Data Protection Impact Assessment for that processing.

There's separate guidance for criminal offence data. You'll need to check the guidance if you plan to keep any of this type of data, but the conditions for processing include:

17. counselling

18. safeguarding of children and individuals at risk

…

31. not-for-profit bodies

This last one is likely to apply, and the others may too.

If you are processing this data, we strongly suggest that you consult the ICO guidance and seek further detailed advice and guidance from a lawyer or data protection professional.

Making Your Decisions

In the first exercise, you'll have identified the data subjects and the different types of data you're collecting about them. Open your completed 'What Data Do You Need' workbook now.

For each of the tables in your data map, you'll need to establish your lawful basis for processing that data. You may find that each row in one table has a different basis. In some cases, you may judge that a single basis for processing applies to all the data in the table.

The Lawful Data workbook contains four template tables, one for each of the four most common lawful bases for processing data used by small charities.

Use each of these tables as a template as you work through, copying it and completing it for each type of data from your data map.

For example, you have trustees. As we've discussed, you process certain identifying information to complete your Charity Commission registration. You also process CVs and further contact information for trustees.

Your data map table may look like this:

Who is it about: **Trustees**

What data about those people?	**Why** do you need it?	Who needs to **access** it?	What will you **do with it**?
Basic Identifying details	Organisation management	Any Internal Public (partly)	Internal communications. Charity Commission register. Companies House register.
Personal contact info (e.g. mobile number)	Organisation management	Trustees, CEO	Internal communications.
CV	Organisation management	Trustees, CEO	Ensure board has balance of skills. Summary on our website.

The lawful basis for processing basic Identifying details is *legal obligation.* Copy the *legal obligation* table from the workbook and complete it for Trustee basic identifying details.

Personal contact information is used to make it a bit easier to stay in touch with Trustees, and to be able to contact them in an emergency. There are several different approaches you could take to this:

1. Consent: you ask Trustees for the information, but don't require it. You explain what you'll do with it, and why. They can withdraw consent if they wish to and remain a Trustee.
2. Legitimate interests: the nature of your organisation means that Trustees may need to be available at short notice in an emergency. You judge that this is legitimate for your organisation—perhaps they are the emergency keyholders for the building, for example. Holding mobile phone numbers is a reasonable way to do this and doesn't impinge on their rights. Alternatives don't work. So, we conclude this is a necessary and reasonable approach.
3. Contract: if you have a Trustee Agreement (a contract) you could consider whether this should form part of that. If so, this could become the basis for processing. You should seek legal advice if you wish to rely on this, as it's not completely straightforward.

This is a rather long-winded weighing up of 'can we process trustee mobile phone numbers?' In most cases you won't need to write down this much detail, just enough to show that you've given the matter some thought and judgement. Where data is more sensitive, or your processing seems like it could be contentious, you may need to give more detail.

In this example, we conclude that consent is the appropriate approach. Copy the *consent* table in the workbook and complete it for Trustee personal contact info.

Finally, we look at our processing of CVs. We carry out the legitimate interests test and conclude that's the most appropriate basis. Copy the *legitimate interest* table and complete it for Trustee CV.

However, you think that *consent* is more appropriate for the CV summaries you want to put on the website. You decide you can add this to the Personal Contact Info table.

Going through all of this makes you realise that you need to update this for your Trustees. Note that you need a 'Trustee Information Sheet' you can ask Trustees to complete. This will need to explain that you are seeking their consent to hold and process the information, what you'll do with it, and that they don't have to provide it. You'll need to store this with their other records to show you have consent.

Next Steps

This exercise may have identified more things you need to think about.

Are you collecting only what you need? Look through your data map once more, and check that all the data you've identified has a lawful basis for processing.

Do you need to carry out any staff training? Data protection is the responsibility of the whole staff, not just one nominated person. The ICO provide the training they carry out for their staff as a series of free videos, at https://ico.org.uk/for-organisations/posters-stickers-and-e-learning/training-resources-for-your-business/. They also provide staff awareness posters and

other resources you can use, available here: https://ico.org.uk/for-organisations/posters-stickers-and-e-learning/

When will you next review your data collection and processing? What will you do with inaccurate data or data you don't need anymore? How will you check the accuracy of your data?

Are there any actions that you identified while doing this? Some of the things you may need to do include:

- updating your privacy notice, or consent collection
- explaining what you're doing somewhere
- knowing what to do if someone wants to access their data
- considering how long you need to keep the data
- drafting a policy
- considering whether you share data with anyone outside your organisation
- planning for what you will do if something goes wrong

How to Store Your Data

Now you are confident you can lawfully process the data you need, how are you going to store it? The Data Protection Act gives you a responsibility to store it securely, and not for too long.

The next steps will be to think about how you store this information and meet your responsibilities to keep it securely. The third and final part in our data journey covers this, with some suggestions about what to think about and pointers in different situations.