



# GDPR Beginner's Guide

## Contents

## Contents

|  |    |
|--|----|
| About GDPR .....   | 2  |
| What is Personal Data .....                                  | 2  |
| Where to start with GDPR and your organisation?.....         | 3  |
| Understand your needs as an organisation .....               | 3  |
| Ask yourself 'Why do I need this information?' .....         | 4  |
| How are you going to keep this data safe? .....              | 7  |
| Be Transparent.....  | 9  |
| Know how to respond to people's Data Protection rights ..... | 10 |
| Responding to a Subject Access Request (SAR) .....           | 11 |
| One month Timeframe .....                                    | 11 |
| Check the information you are sending .....                  | 12 |
| Refer to your privacy notice and keep records .....          | 13 |
| Know how to identify and handle data breaches .....          | 13 |
| Check if you need to register with the ICO .....             | 15 |
| Set reminders to keep your GDPR up to date .....             | 15 |

## About GDPR

The General Data Protection Regulation (**GDPR**) took effect on the 25th May 2018 across the European Union. It regulates how any organisation, including charities, should handle data. Although it began as European Union law it was incorporated into the UK's Data Protection law after the completion of the Brexit transition period.

It is legislation that protects EU and UK citizens' personal data while also affecting charities that deal with such data. These laws will apply if your charity or not-for-profit requests, receives or stores personal data from EU and UK Residents.

The ICO (**Information Commissioner's Office**) is the GDPR Regulator in the UK, and charities and not-for-profit organisations are treated the same as any other organisation since although they do not collect data for profit they are still prone to data breaches and privacy violations.

## What is Personal Data

Under UK GDPR, personal data is defined as any information relating to an identified or identifiable natural person. This includes both direct and indirect identification methods.

### Direct Identifiers:

- Names
- Addresses
- Phone Numbers
- Email Addresses

### Indirect Identifiers:

- Identification Numbers
- Location Data (e.g. IP Address)
- Online Identifiers (e.g. cookies)

There are some types of personal data that are likely to be more sensitive known as **special category data** under the UK GDPR. This includes personal data revealing or concerning:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where used for identification purposes)
- Health
- A person's sex life
- A person's sexual orientation

If you're processing any of these types of data, you should give particular consideration to how and why the data is used and make sure you only use it when it's absolutely necessary.

## Where to start with GDPR and your organisation?

### Understand your needs as an organisation

The first step to thinking about GDPR and your organisation is to understand what data you already hold and/or what data you plan to collect. It is helpful in this exercise to write down everything you can think of as well as all of the places that you hold this information.

#### EXAMPLE:

Jane runs a local community project that puts on special interest sessions for people who are isolated. In order to advertise these groups she sends her members emails and WhatsApp messages to encourage them to take part.

In order to do so she collects their Names, Phone numbers and Email Addresses. She keeps the information on a spreadsheet on her computer but also has some of this information on her phone.

She also has a list of volunteers who help her run the sessions. She sends resources and materials to the volunteers home addresses from time to time. She keeps this on a separate spread sheet on her computer.

She is planning to run some more targeted sessions in collaboration with a local multicultural organisation but would like to know the ethnic origin of those who might be involved to know what sorts of sessions she should run.

Her Direct Identifiers are: Names (Participants and Volunteers),  
Addresses (Volunteers), Phone Numbers (Participants and Volunteers),  
Email Addresses (Participants and Volunteers)

Her Special Category data will be Racial or Ethnic Origin (Targeted sessions with local multicultural org.)

She keeps the information on her phone and her computer.

## Ask yourself 'Why do I need this information?'

In order to hold someone's personal information, it is important that there is legitimate interest. Legitimate interest is broken down into reflective questions by the ICO.

- Is there a reason to process the data in the first place?
- Is data processing required for that purpose?
- Is the legitimate interest at odds with the individual's interests, rights, or freedoms?

The data you are collecting must be collected for a specific purpose and the data must be legitimately required for that purpose. In the example, we gave you above Jane collected names, phone numbers and addresses to keep her members informed of when the sessions were happening. This is a legitimate use for this data, as without it she could not keep in contact. However if she had collected names, phone numbers, addresses and political affiliation it would be argued that she didn't need her members political affiliation to keep them informed. There would not be a legitimate reason to hold this data.

We understand that in order for Jane to get in touch with her members she needs to know who they are and have a way to contact them.

### EXAMPLE:

Let's imagine that instead of Jane using the information she has collected to contact her members, she uses it to keep a register of who attends her sessions. Does Jane need to collect an email and phone number in order to keep a register of who attends her sessions?

No. The reason you collect contact information is to be able to contact someone. Collecting contact information for a register would not be considered required for that purpose.

The last part of legitimate interest asks if collecting the data would be at odds with the individual's interests, rights or freedoms. Below is a summarised list of individual's rights in relation to data protection:

- **Right to be informed**

Individuals have the right to be informed about the collection and use of their personal data.

- **Right of access**

Individuals have the right to access and receive a copy of their personal data and other supplementary information.

- **Right to rectification**

The UK GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.

- **Right to erasure**

The UK GDPR introduces a right for individuals to have personal data erased.

- **Right to restrict processing**

Individuals have the right to request the restriction or suppression of their personal data.

- **Right to data portability**

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

- **Right to object**

The UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.

- **Rights related to automated decision making including profiling**

The UK GDPR has provisions on:

- Automated individual decision-making (making a decision solely by automated means without any human involvement).
- Profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

### **EXAMPLE:**

Jane has decided in order to get a jump on her new collaborative project with the local multicultural organisation, she will start to collect the racial or ethnic origins of her members in order to get an idea of what sort of projects she may want to consider. She decides that she will collect this data on her membership spreadsheet. She has decided not to tell any of her members about these projects just yet as she does not want to get her member's hopes up if it does not pan out.

Although Jane has a legitimate use for this data to inform the creation of new services – Jane is now also holding special category data that she hasn't asked for. She has infringed on their right to be informed. Indirectly, by not being informed, her members cannot object to the data being held or restrict its use.

## How are you going to keep this data safe?

Whenever someone shares their personal details with you, they trust you to protect this information. If this data is lost, damaged or falls into the wrong hands, it results in a Personal Data Breach, which can have harmful consequences for both you and those affected.

When we consider data security, we often focus on digital protection and preventing unauthorised access to our data. However, it's important to remember that we have a responsibility to safeguard information both digitally and physically. The ICO have **12 Tips for data security** that are helpful when considering how to keep data secure.

[Data security: quick wins | ICO](#)

### Take care when printing and photocopying

If you're printing or photocopying on a shared printer, check you've left nothing behind before returning to your desk. Put a sign at the printer to remind staff to collect all of their paperwork, including original copies.

### Double-check letters before posting them

Picking up two letters instead of one is an easy mistake to make if you're working your way through a stack of them. Ask a colleague to double-check that the right letter is in the right envelope before you post them. Or you could use place-markers to help you spot where one letter ends and the next one starts.

### Include a return address on your envelopes

If you send a letter and it ends up at the wrong address, the person who receives it by mistake can return it without opening it if you put a return address on the back.

### Disable autofill in your email settings

If people's email addresses come up automatically when starting a new email message then you have autofill enabled in your settings. While this

tool might save time, it could cost you if you send an email to the wrong person by mistake, so it's a good idea to disable it.

### **Close your messages when screensharing or presenting online**

If you're doing an online presentation to a group of people, the last thing you want is for a personal message or email to pop up. Close your emails and messaging services before sharing your screen with others.

### **Lock your screen when you're away from your desk**

Encourage your staff to lock their screens when they're away from their desks, and lead by example by locking yours too. This helps prevent others from seeing information they're not authorised to see.

### **Don't let your staff share passwords**

Staff should all have their own separate log-ins and passwords. They shouldn't share their passwords with each other. This increases the risk of an unauthorised person seeing, altering or using personal data.

### **Send electronic documents securely**

If you need to send electronic documents, consider encrypting or password-protecting them. This reduces the risk of the wrong person being able to access the documents.

### **Send passwords to protected documents in separate emails**

If you're sending password-protected electronic documents, make sure you send the password separately.

### **Keep your IT systems up-to-date**

You can reduce your risk of cyber threats, such as hacks of computer systems, by making sure you regularly install security updates.

### **Think before you speak**

Don't accidentally reveal something about someone in passing, such as telling a colleague why someone is off work.



## Be aware of your surroundings

Be careful what you say and what documents are open on your screen when people are around you, particularly if you're in a public place where people can easily see you and overhear your conversations.

You should retain personal data only for as long as necessary. Data protection laws don't specify exact time limits, as this varies based on your circumstances. Consider the original purpose for collecting the personal information and your lawful basis for processing it. You need to evaluate and justify the duration for which you keep the data, depending on your reasons for holding it. It is good practice to review the data you hold on a regular basis and put limits in place as to when to dispose of information that is no longer pertinent.

### EXAMPLE:

**John is reviewing their membership data. They have been running the project for a long time and have data that goes back beyond 5 years. John suggests to the organisation that they remove personal data records for anyone who has not be in touch with the organisation for 2 years. This gets approved. This enables him to remove a number of records that are no longer serving any purpose and thus reducing their data risk.**

## Be Transparent

When collecting personal data you must be up front and honest about what it is you need their data for. As above it is helpful to know exactly why you need to keep the data in the first place, and in understanding this it is far easier to communicate that need to people you are collecting from. Being clear and upfront about what data you are collecting and why also provides comfort to those offering the data to know it's in good hands.

A helpful and formal way of putting this information together is by using a privacy notice. A privacy notice lets people know what information you have and what you'll do with it.

The ICO have their own privacy notice generator that you can use to quickly and easily generate the information that you need that is bespoke to your organisation. This tool will make sure that your organisation is compliant with the law and shows that you care about their information.

[Create your own privacy notice | ICO](#)

## Know how to respond to people's Data Protection rights

Individuals have rights concerning their personal information. They can request its deletion, challenge its accuracy and object to its use.

Additionally, they can ask for a copy of their personal data, known as a Subject Access Request (**SAR**).

Implementing a process for managing these rights requests can save you time in the future. It's beneficial to have this in place, even if you haven't received any requests yet. You should choose an individual who will be the Data Protection Lead who understands your organisation's process for dealing with these requests.

When a request comes in, it is always important to know who you are dealing with and confirm they are who they say they are. You can ask questions that only they would know the answer to. This can be appointment details or how they were involved with you as an organisation. As a last resort you could ask them to provide identification, but remember the request should be proportionate to the situation. If you are contacted on someone's behalf, a friend or a relative perhaps, check the validity of that request before going ahead. Having a written confirmation or evidence of written authority is a good way to confirm this.

## EXAMPLE:

John receives a Subject Access Request (SAR) from a member's brother. They want to confirm that their contact details and their current address are correct. John has never met the brother and, until this interaction, wasn't sure if he knew that the member even had a brother. John asks for the brother for the member to get in touch to confirm that this request is genuine before proceeding.

## Responding to a Subject Access Request (SAR)

A SAR is a request from a person, or from a third party on behalf of a person, to receive information about which of their personal details you hold. It can be a request for a complete picture or a request for specific information. Individuals have the right to access and receive a copy of their personal data and any other supplementary information.

You have one calendar month to gather the necessary information and send it to the relevant person. If you need to verify their ID or request additional information, you can wait for their response before starting the one-month countdown. However, you should request any additional information as soon as possible.

### One month Timeframe

There are three key points to remember about the one-month timeframe:

- The day you receive the request doesn't need to be a working day. For instance, if you receive a request on Saturday 7 March, you should respond by Tuesday 7 April.
- If the SAR's due date falls on a weekend or public holiday, you have until the next working day to respond. For example, if you receive a request on 25 November, you should respond by 27 December.
- You cannot add extra days when the calendar month is shorter. For example, if you receive a request on 31 January, you should respond by 28 February.

It is important that you understand what information is being requested and that you and the requester are on the same page. You can save a lot of time and energy understanding specifically what they are looking for and it is okay to ask them, so long as you are asking what questions and not why questions.

## Check the information you are sending

Remember that just as they have the right to see their own personal data you still have the obligation of protecting other people's. Make sure that you are only sending personal data relevant to the request. Redacting can be used to conceal other people's personal information and it can be useful to learn how to correctly redact information sending, especially if you are sending digital copies.

It is also important to consider the impact of releasing data about other people if the information that is being requested is closely linked. It is important to remember individuals all hold independent rights. Here is a useful example from the ICO website that clarifies this.

### EXAMPLE:

**Samira is an employee who has made a SAR for her personnel file. In her file is a complaint a colleague, Tom, made about Samira. Although the information in the complaint is about Samira, if you release it to her, it might identify Tom. You need to weigh up Samira's right to her personal data, against giving out information about Tom without good reason.**

**There are three options here:**

- **If Samira knows all about the complaint, what was said and who said it; you could give her the information as it is, without redacting Tom's details.**
- **If Samira doesn't know about the complaint and wouldn't guess that it came from Tom, you could supply the details of the complaint, but redact Tom's name or any other identifying information.**

- If Samira doesn't know about the complaint but would guess that it came from Tom, whether his details were redacted or not; you may need to consider whether it's necessary to get Tom's consent.

It's a balancing act between making sure Samira is given the data she's entitled to, and not disclosing Tom's details if you don't have to.

If you think releasing the information to Samira may mean that there would be a negative impact on Tom, then you could consider withholding this piece of information altogether. If you do this, you should make a note of why you withheld it.

From <<https://ico.org.uk/for-organisations/advice-for-small-organisations-new-structure-work-not-to-be-put-live/subject-access-requests-sar/how-to-deal-with-a-request-for-information-a-step-by-step-guide/>>

## Refer to your privacy notice and keep records

Alongside the personal information you should also send privacy information. This should include why you hold people's data, how you got it, how long you intend to keep it, who you might share it with and how they can ask for it to be changed or deleted. You should know most of this information and it can be clearly laid out in your privacy notice. Make sure to include this in your response. When you are ready to send the information keep a record of what you have sent them in case you need to refer to it again.

## Know how to identify and handle data breaches

It is important to recognise that there are many ways that data breaches can occur. Some examples can be:

- Information is lost – Laptops or phones with personal data on are misplaced or stolen.
- It can be accidentally destroyed – Someone shreds or deletes the wrong file meaning the data is no longer available
- Information can be altered without proper permission
- Accidentally disclosed – Information could be sent to the wrong person.

If you identify that there has been a data breach the key things to remember are:

- You have 72 hours to report a personal data breach if it meets the threshold for reporting.
- It is important to start logging and recording all the information as you go.
- Find out what has happened and pull all the details together quickly.
- Try to contain the breach so that you protect those who will be impacted
  - If a document is sent to someone by mistake, ask them to delete it, send it back securely or have it ready for you to collect
  - If have lost information try and retrace your steps to find it.
  - If you have lost a device, take steps to remotely wipe the device if that is an option
  - If you have had a cyber incident make sure you change all passwords as quickly as possible.
- Assess the risk – What is the harm that could be felt by the person or peoples data you have lost. Understand what the impact could be to those involved to understand the seriousness of the situation. Is it a simple mix up or does it present for example safeguarding issues, risk of identity theft or any form of significant distress. The ICO have a guide to help organisations understanding the risk around personal data which can be found here: [Understanding and assessing risk in personal data breaches | ICO](#)
- Act to protect those effected. If you can, try to give people clear, practical advice on how they can protect themselves, and let them know what you're able to do to support them. But if you don't think

there's much risk to them, it's okay not to bring up the incident. If you do believe there is a high risk you have a lawful obligation to let them know.

- If you are required to report it to the ICO you should now at this point submit your report to them. It is possible to report online using their website. [Report a data breach online form | ICO](#)

## Check if you need to register with the ICO

Most not for profit organisations are exempt from registering with the ICO although CIC's need to be aware that the exemption does not cover them. It is well worth using the ICO's self-assessment tool to know if you need to be registered or not.

### [Self-assessment tool](#)

If you are exempt from registering with the ICO you are still bound by the laws around GDPR and still need to take steps to ensure that you are compliant.

## Set reminders to keep your GDPR up to date


GDPR is an ongoing process and your organisation will need to regularly assess your GDPR needs over time. This might include updating your privacy notice, checking your retention schedule, or reassessing what data you are collecting. Make it a priority to put reminders in your organisations calendar to remember to revisit GDPR and keep yourselves up to date.

## ***Need more support?***

Wirral CVS is here to help your organisation grow, develop and succeed. Whether you're just starting out or strengthening your foundations, our Development Team can provide one-to-one guidance, training, resources and advice tailored to your needs.

## **Contact us to book a support session**

 **Email:** *info@wirralcvs.org.uk*

 **Phone:** *0151 433 3371*

 **Website:** *www.wcvs.org.uk*

## ***More resources available at:***

**[www.wcvs.org.uk/support](http://www.wcvs.org.uk/support)**

Including templates, guidance and policy tools across governance, finance, safeguarding, volunteering and more.

## ***Disclaimer***

**[www.wcvs.org.uk/support](http://www.wcvs.org.uk/support)**

This document is provided for general guidance only. It does not constitute legal advice. We recommend seeking professional support where required.

