# How to ensure your organisation is GDPR ready

*This guide is designed to act as an introductory overview. We recommend that key decision makers refer to the full guidelines and other helpful resources, which can be found on page 3.*

---

**Top tip: Start planning as soon as possible – do not leave it to the last minute.**

---

## 1. Raise awareness

Make sure key decision-makers in your organisation are aware of the new legislation and have plenty of time to act.

## 2. Formulate a plan

Identify which parts of the GDPR will have the biggest impact on your organisation. Start with these areas.

- Plan and allocate resources to each task. Set realistic timescales.
- Communicate your plans across the entire organisation: everyone (including volunteers) should know about the changes and be fully on board.

## 3. Data Protection Officers

The responsibility for data protection compliance must be formally designated to someone in your organisation. They must have the support, knowledge and authority to carry out this role effectively.

- If this requirement cannot be met, it must be outsourced externally.

## 4. Take stock of your data

Map all of the personal data you hold, where you got it from, and who you share it with.

- VCSE sector organisations are strongly encouraged to carry out a full data audit, across the entire organisation.
- To comply with the GDPR's accountability principles you must have effective policies and procedures in place relating to data collection and protection practices.

## 5. Communicate clearly with your contacts

Review existing privacy notices and build on them using GDPR guidelines:

- You will now need to explain your legal basis for processing the data, your data retention periods and outline individuals' rights to complain to the ICO if they think you are not handling data legally.

## 6. Protect individuals' rights

This includes the right to access, delete and correct data your organisation holds. If you are already compliant with the Data Protection Act the transition should be quite straightforward. However, there are 'significant enhancements' to be aware of.

- Check your procedures and identify whether your current systems allow you to easily locate data, should a request occur.

## 7. Subject access requests

The GDPR could potentially have a huge impact on administration time and costs, if your organisation handles large volumes of requests. Even if it doesn't, you will need to plan how your organisation handles requests according to the new guidelines. For example:

- You will now have a month to comply, instead of 40 days.
- There are also changes to whether you can charge for requests (in most cases you can't)
- You will also need to provide additional information to those making requests.

## 8. Your legal basis for processing personal data

Organisations must identify and document their legal basis for all types of data processing. You will also need to explain your legal basis for processing personal data in your privacy notice. Some people's individual rights will change depending on what that legal basis is.

## 9. Consent

Every organisation will need to review the way it seeks, gets hold of and records consent for use of personal data. Where previously people could 'opt out' once you have their data, they must now 'opt in' before their data can be used.

- Consent must be clearly informed, and given freely and specifically. There must be a positive indication of consent – you can't infer it through silence, pre-ticked boxes or inactivity.
- Your organisation must be able to prove that positive consent was given.

## 10. Children

If your organisation collects information about children (aged under 13, in the UK), you will need to put systems in place to verify their ages and seek parental/guardian consent.

- Your privacy notice must be written in language that children understand.
- Given consent must be verifiable.

## 11. Data breaches

Some charities are already required to notify the ICO if there is a data breach. The new GDPR will make this rule apply to all charities.

- Ensure you have the right procedures in place in the case of a data breach, and that all staff are aware of them.
- Assess the types of data you are holding, indicating which would fall within the notification requirement.
- Know what steps to take: not all breaches will need to be reported to the ICO, however in some cases you must notify individuals whose data has been breached.

## 12. Data Privacy Impact Assessment (DPIA) guidance

There is new ICO guidance on DPIAs, which in most cases are only required in high-risk situations. You should read these and plan how to implement them in your organisation, and in situations where your data is linked with other organisations. A privacy by design and data minimisation approach will be a legal requirement under the GDPR.

## 13. International charities

International charities need to determine which data protection authority they fall under. This is usually the place where the organisation's main administration is based.

## Useful resources

Watch the Information Commissioners' Office (ICO) video guide.

Fundraising and data protection: A survival guide for the uninitiated (2040 Training)

GDPR: The Essentials for Fundraising Organisations (Institute of Fundraising)

Personal information and fundraising: Consent, purpose and transparency (Fundraising Regulator)

Data Protection self-assessment toolkit (ICO)

Consent self-assessment tool (Fundraising Regulator)

---