GETTING READY FOR GDPR

10 STEP ACTION PLAN

Institute of Fundraising

Small Charities Coalition

1 UNDERSTAND WHAT GDPR MEANS FOR YOU

The General Data Protection Regulation is a new EU Law that will apply from 25 May 2018. It covers the control and processing of personal data – so for charities that will include the information you hold and use about supporters, staff, volunteers, beneficiaries & service users. You need to know about your duties and the rules you'll need to follow as well as privacy rights for individuals.

TOP TIP:
For info on the rules and changes.
Take a look at 'GDPR: What you need to know'

2 KNOW WHERE YOU'RE STARTING FROM

GDPR does bring in new rules on data protection, but data protection isn't new. So rather than changing everything to start again, it's important to know how you are currently processing data & review the systems you have in place. You need to know your starting point before you start planning your journey to GDPR compliance.

TOP TIP:
Undertake an 'audit' to review your current practices and data protection policies

3 DISCUSS WITH YOUR TRUSTEE BOARD

Every charity's trustee board has a responsibility to make sure the organisation is operating according to the law. Agree a strategy at Board level to set your approach. You might need more resources or budget to ensure you're compliant and will also need updated data protection policies which should be signed off by the Board.

TOP TIP:
Trustees should be involved in the process but that doesn't mean they have to take EVERY decision – work out what the right level of delegation and oversight is for you.

4 ADOPT AN ORGANISATION-WIDE APPROACH

Data protection isn't just about fundraising – it's all the processing of personal data that your organisation does, including campaigning, direct marketing, or service delivery. It's likely that changes will impact across every part of an organisation, so involve colleagues, including IT & your database officer/manager if you have one.

TOP TIP:
Set up a working group with relevant people across your organisation so that you can agree a 'whole organisation' approach.

5 SEEK EXTERNAL SUPPORT WHERE YOU NEED IT

If you're new to all this it might feel pretty overwhelming. Some organisations might have a data protection officer or in house expert, but others won't. There are lots of data protection experts or law firms around who offer a range of advice (some of it free!) – talk to one if you think you need to get some more in-depth support.

TOP TIP:
Finding the resource or budget might be hard, but compliance with GDPR isn't optional. External support at the right time can really help you get ready.

6 DIRECT MARKETING: CONSENT OR LEGITIMATE INTEREST?

For electronic communications (emails, texts, and telephone numbers listed on the TPS) you will nearly always need an individual's consent to send them direct marketing.

For postal and telephone numbers (not on TPS) organisations can get consent from individuals as above, or you can seek to satisfy the 'legitimate interest' basis. Remember though, that a charity's legitimate interest must not outweigh the rights of the individual – you'd need to carry out a 'balancing exercise' to take into account the reasonable expectations of the individual and ensure their privacy rights aren't being overriden.

TOP TIP:
Decide on your approach to direct marketing that is most appropriate for you – for more information on consent and legitimate interest go to GDPR Essentials

7 MANAGE PERSONAL DATA PROPERLY

The amount that the Information Commissioner's Office (ICO) can fine organisations for breaches of data protection has been increased. You also need to make sure you have the right procedures in in place to detect, report and investigate a personal data breach.

TOP TIP:
Know what constitutes a personal data breach – if one happens you'll have 72 hours to report it to the ICO.

8 PREPARE TO BE ABLE TO RESPOND TO REQUESTS FROM INDIVIDUALS

GDPR brings in stronger rights for individuals. This means people can make subject access requests at any time to check the data that you're holding about them and what you're going to do with it. There is also a new 'right to be forgotten' where people can request the removal of personal data. Data has to be kept up to date and accurate so think through how you will make sure you are keeping data for no longer than is necessary.

TOP TIP:
Plan how you're going to handle any requests from individuals so you can respond quickly.

9 DON'T PANIC

GDPR is an evolution, not revolution. The Data Protection Act has already required that organisations process personal data fairly and lawfully for years. Take GDPR as an opportunity to review how you process data already and make the changes needed so that you're ready for May 2018 and beyond.

TOP TIP:
Action you take now will influence how your organisation processes personal data in the future. Think it all through and make the right decisions for your charity weighing up all of the relevant factors.

10 THIS IS ABOUT PEOPLE, NOT JUST COMPLIANCE

This isn't just about complying with the law: at its heart, data protection is about keeping personal data safe and being fair in how work with individuals. GDPR doesn't stop you fundraising, but it does mean you need to be responsible in how you fundraise.

TOP TIP:
Think about this from the individual's point of view – always be clear about how you want to use their data and give people the right opportunities to express their choices.

For more information and resources go to **www.institute-of-fundraising.org.uk/GDPR**