1 GDPR & Charitable Fundraising: Introduction

Produced by: Institute of Fundraising; FUNDRAISING REGULATOR

Reviewed by: ico. Information Commissioner's Office

An Introduction

What is the GDPR?

The General Data Protection Regulation (GDPR) is a new law which will replace the current Data Protection Act. Every organisation in every sector that processes personal data will have to be compliant with GDPR – this isn't a 'nice to have', it's a fundamental legal responsibility of every charity to ensure that they have the right policies and procedures in place so that they are being run properly and are taking individuals' rights seriously.

When does GDPR apply?

GDPR becomes effective on 25th May 2018. The UK Government is also legislating to make sure that GDPR passes into law before the UK leaves the European Union.

> [Top tip]: *Don't wait until then to start thinking about GDPR – organisations are expected to be ready by 25th May so you need to be thinking about how you will be compliant and making any changes and decisions now.*

However, don't panic - data protection legislation has been around for years and the GDPR is an update of existing requirements rather than something completely out of the blue. The Information Commissioner has emphasised that GDPR compliance should be seen as a journey requiring ongoing effort rather than a race ending on 25 May 2018. While the ICO will be regulating against GDPR from this date, the Commissioner is clear that "those who self-report, who engage with the ICO to resolve issues and who can demonstrate effective accountability arrangements can expect this to be taken into account when we consider any regulatory action".

> [Top tip]: *So, understand what's different, check how compliant you already are, and put in place a plan and process to make changes where needed.*

Key definitions

Personal data: any information relating to a living individual who can be directly or indirectly identified from it. This includes name, address, contact details but could also include two or more non-specific pieces of information that when combined could identify specific individuals, including, for example, a combination of gender, birth date, geographic indicator and other descriptors.

Special categories of personal data: data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric information, health and a natural person's sex life or sexual orientation.

www.ico.org.uk

Visit for more information on each lawful basis

Data controller: a controller determines the purposes and means of processing personal data – organisations will be 'data controllers' (e.g, charities, banks, companies) when they hold and use the data of customers and clients.

Processing personal data: means doing something with personal data – this includes keeping records, using data for direct marketing, carrying out a contractual obligation among others. A fuller definition of "personal data" can be found at https://ico.org.uk/

What does this mean for charities and charitable fundraising?

Charities will be 'data controllers' in a number of ways, including:

- As an employer processing the personal data of employees, trustees and volunteers.
- As a provider of personalised services to beneficiaries and clients.
- As a fundraising or campaigning organisation that has donors and supporters.

Individual fundraisers may also be data controllers where they are acting independently of a charity in processing data (for example, community fundraisers who may hold supporter details while carrying out a campaign "in aid of" a charity but not acting in an official capacity on behalf of that charity – See ***Briefing Paper 3*** for further details).

How can we process personal data lawfully?

GDPR doesn't stop charities campaigning, fundraising, or providing services to beneficiaries. It just means that when a charity does so it has to do it fairly and lawfully, being transparent and respecting individuals' privacy rights.

Charities can process personal data (e.g, send marketing materials, contact service users, store employee records), but it has to be done according to a 'valid lawful basis' that GDPR sets out. There are six available bases for processing:

(a) Consent: you can show that an individual has performed a clear affirmative action (such as saying "yes" to a question or ticking an opt-in box) to allow 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 the interests or rights and freedoms of the individual override those interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

[Top tip]: *It's important for charities to understand that no single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual. You must determine your lawful basis before you begin processing the data and you must include your lawful basis in your privacy notice. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.*

Individual rights under GDPR

As well as setting out the different bases for being able to process personal data, the GDPR also includes a number of rights for individuals which charities need to recognise and act upon.

– The right to be informed

– The right of access

– The right to rectification

– The right to erase

– The right to restrict processing

– The right to data portability

– The right to object (including objecting to direct marketing)

– Rights in relation to automated decision making and profiling.

For more information on individual rights go to https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

What else do charities need to know?

Accountability and governance are important principles of GDPR. What this means is that charities have an overall duty to demonstrate that they are complying with the requirements of GDPR. Each charity will need to put into place proportionate governance measures, including reviewing and approving internal policies, documenting activity, keeping records of data processing, and undertaking data protection impact assessments where necessary.

> [Top tip]: *Think about it from a regulator's point of view. If anyone were to question your practices, how would you be able to prove that you were being compliant and justify the decisions that you take?*

There are also requirements around data security and international transfers, and a duty to inform the ICO within 72 hours (including weekends or out of working hours) if you have a data breach. In some circumstances, you will also need to inform the data subject. The risks of non-compliance include fines, reputational risk, and personal law suits from individuals so it's important to get this right!

For more information on all your duties and potential enforcement action go to www.ico.org.uk

Also – don't forget that charities need to follow the Code of Fundraising Practice for the standards required of charity fundraising set by the Fundraising Regulator. This will include relevant parts of GDPR, but also include further requirements that charities need to follow in their fundraising activity.

A checklist for charities:

– Do you know the GDPR requirements and have you thought about what it means for your charity and the personal data you process?

– Have you undertaken a review or audit of the data you currently hold and your policies and procedures? What do you need to update or change?

– Have you thought about which lawful basis you will use for different data processing purposes and do you understand how to use each one fairly?

– Are you aware of individuals rights and would you be able to respond appropriately to any requests from them regarding their personal data?'

– Have you thought about all the different processing your charity does (for example, volunteering, campaigning, fundraising) and do you have an organisation-wide approach?

– Are your Customer Relationship Management (CRM) system and database able to appropriately and securely keep data?

– Are you being accountable – do you have a data protection policy in place and are you documenting decisions, and training staff?

Signposting and resources:

ICO

Guide to the general data protection regulation
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Fundraising Regulator

Code of Fundraising Practice
https://www.fundraisingregulator.org.uk/code-of-fundraising-practice/code-of-fundraising-practice-v1-4-310717-docx/

Personal Data: consent, purpose and transparency
https://www.fundraisingregulator.org.uk/information-registration-for-fundraisers/guidance/personal-information-fundraising-consent-purpose-transparency/

IoF

GDPR: The Essentials for Fundraising Organisations
https://www.institute-of-fundraising.org.uk/library/gdpr-the-essentials-for-fundraising-organisations/

Supported by:

CHARITY COMMISSION FOR ENGLAND AND WALES · The Charity Commission for Northern Ireland · Scottish Fundraising Standards Panel (Legal, Open, Honest, Respectful) · NCVO · Cyngor Gweithredu Gwirfoddol Cymru WCVA Wales Council for Voluntary Action · nicva