Steps to Recovery

GDPR guidelines for small charities and organisations

What is the UK GDPR?
The UK GDPR sets out requirements for how organisations need to handle personal data. It is part of the data protection landscape, which also includes the Data Protection Act 2018 (the DPA 2018).

Why does GDPR apply to us, a small charity organisation?
GDPR applies to your organisation because you will undoubtedly have personal data on individuals: service-users, staff and volunteers, as well as supporters and patrons. The GDPR law applies to any 'processing of personal data', and will affect most businesses and organisations, whatever their size.

What is personal data?
'Personal data' is any information relating to an identifiable person who can be identified from the information (directly or indirectly, for example, name, address, age - or a combination).

What is special category data?
As well as personal data, organisations may also want to collect special category data (which includes, political leaning, ethnicity, health, sexual orientation). Special category data is personal data that needs *more* protection because it is sensitive.

For this reason... If you are a small organisation and only need this type of information for needs assessment and evaluations, we recommend you have a policy of only collecting this data anonymously. This way, special category data will only need to be one clause of your GDPR policy.

If special category data *is* particularly relevant for your organisation, read more at the ICO website.

1.

Step-by-step of creating an GDPR policy

As a small charity or community organisation what do I have to do to ensure we comply with the UK GDPR?

2. **Adopt a written policy** - start with a statement setting out your approach to data protection in your charity. Then follow steps 2-6. See the template below.

3. **Specify who is responsible:** assign someone responsibility for overseeing charity data protection and note this in your written policy.

4. **Establish data collection and maintenance procedures:** review your systems to ensure the data you collect is:
    a. Just the data you need (e.g. email addresses and names, but not home addresses and telephone numbers), and
    b. Accurate and kept up-to-date.

   Note the procedures down in your policy. A data collection policy might involve surveys or registering participants at events.

5. **Establish a procedure for responding to requests:** Article 15 of GDPR grants people the right to ask for a copy of the personal data that you have on them. These 'data subject access requests' are your responsibility as a 'data controller.' Decide how these will be processed and write a line on this in your policy.

6. **Establish disposal procedures** - include within your written policy details about how you will ensure that unused and out-of-date data will be safely disposed of. For example, when someone has requested not to receive correspondence from your organisation anymore, have a reliable procedure in place to ensure their name and contact details are permanently removed from all your databases.

7. **Establish procedures for maintaining security** and include them in your written policy. These can be one or two simple steps you'll take to ensure the systems you use to process data are secure. For example, you may only have one or two members of staff/volunteers who can access your database of contacts.

8. **Register with ICO** here as an organisation that processes personal data. ICO offers a self-assessment tool if you're not sure whether you need to register and pay.

9. **Train your staff** on how to keep to your GDPR policy - and keep staff up to speed on practical data protection issues like clearing out old information, keeping their access passwords secure, etc.

10. **Write a privacy notice:** whereas a policy is more of an internal document, for funders. A privacy notice is a short statement summarising your policy for service-users and the public.

Your privacy notice should be clear on your website and all the forms through which you collect personal data. Here's a Privacy Policy Template

Template

Data Protection Policy

[Insert charity name]

Last updated: *[date]*

Definitions

Charity	means *[insert charity name]*, a registered charity.
GDPR	means the General Data Protection Regulation.
Responsible Person	means *[insert name of person responsible for data protection]*.
Register of Systems	means a register of all systems or contexts in which personal data is processed by *the Charity*.
Data Subjects	Means the person in which the data is on.
Processing	means anything you do with data; including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.

1. Data protection principles

The Charity is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely

for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2. **The following general provisions apply:**
    a. This policy applies to all personal data processed by *the Charity.*
    b. The Responsible Person shall take responsibility for *the Charity*'s ongoing compliance with this policy.
    c. This policy shall be reviewed at least annually.
    d. *The Charity* is registered with the Information Commissioner's Office as an organisation that processes personal data.

3. **Responsible persons:**
    a. *[insert name of person responsible]* is responsible for overseeing data protection procedures within *the Charity.*
    b. *The Responsible Person* will make sure that this policy is enforced throughout the organisation.
    c. Although *the Responsible Person* will oversee overall execution of GDPR, it is everyone's responsibility to comply with GDPR. Because of this, *the Charity* runs *[insert frequency of training sessions]* training sessions on GDPR for staff and volunteers.

3. **Lawful, fair and transparent processing:**
    a. To ensure its processing of data is lawful, fair and transparent, *the Charity* shall maintain a Register of Systems. Individuals have the right to access their personal data and any such requests made to *the Charity* shall be dealt with in a timely manner.
    b. The Register of Systems shall be reviewed at least annually.

4. **Lawful purposes**
    a. All data processed by *the Charity* must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
    b. *The Charity* shall note the appropriate lawful basis in the Register of Systems
    c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
    d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in *the Charity*'s systems.

5. **The Register of Systems is as follows.**

    a. **Data minimisation procedure:**

i. *The Charity* shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, by *[add considerations relevant to the Charity's particular systems]*

b. Data accuracy procedure:

i. *The Charity* shall take reasonable steps to ensure personal data is accurate, including *[add one or more considerations relevant to the Charities particular systems].*

ii. Where necessary for the lawful basis on which data is processed, personal data will be kept up to date. *[If desired, add one or more considerations relevant to the Charity's particular systems here]*

b. Procedure for responding to requests:

i. All staff will report data subject access requests back to the Responsible Person, who will ensure the request is dealt with appropriately and lawfully. *[If desired, the Charity can specify the following…*

ii. On receipt of a request, the Charity will provide the following information:

1. *The categories of personal data involved*
2. *The purpose for processing*
3. *Who also received the data*
4. *How long you intend to store the data*
5. *When and how to ask you for the right to erasure, restriction of processing, and correction of data*
6. *Their right to lodge a complaint to the Data Protection Authority*
7. *How you accessed data you didn't collect from the source]*

c. Procedure for data disposal:

i. All data that is unused and out-of-date data will be safely disposed of, under the supervision of the Responsible Person. *[If desired, add one or more considerations relevant to the Charity's particular systems here]*

d. Security procedure

i. *The Charity* shall ensure that personal data is stored securely using regularly-updated secure software. *[If desired, name the programme on which you will store contacts]*

ii. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

iii. When personal data is deleted this will be done safely such that the data is irrecoverable.

iv. Appropriate back-up and disaster recovery solutions shall be in place.

6. Privacy notice

a. *The Charity* has a privacy policy that is clearly presented on our website, will be available on any e-communications, and can be requested on demand.

7. Breach

a. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, *the Charity* shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).