# GDPR Factsheet for CoS Groups

Disclaimer: The information provided in this factsheet and any policies provided here or on our website are intended for guidance only. They are not a substitute for professional advice and we cannot accept any responsibility for loss occasioned as a result of any person acting or refraining from acting upon it.

**We strongly recommend that you seek advice from your local CVS or Volunteer Centre regarding any aspect of the GDPR that you are unsure about and its implications for your group.**

## What is the GDPR?

- GDPR stands for General Data Protection Regulation.
- It comes into force on 25 May 2018
- The new regulation governs how organisations handle and protect personal data

## Who does this apply to?

- If you collect email addresses from supporters in order to send them news and information about your group
- If you take pictures that will be stored somewhere (including online)
- If you collect personal data about volunteers or staff
- If you collect personal data about sanctuary seekers / service users

## What counts as personal data?

- Personal data is any information about an individual that can be used to identify them. Examples include:
  - Name
  - Address
  - Phone number
  - Email address
  - Photos
  - Bank details
  - Computer IP address
- Sensitive personal data is a separate category of data with stricter rules:
  - racial or ethnic origin
  - political opinions
  - religious or philosophical beliefs
  - trade union membership
  - genetic or biometric data
  - data concerning health
  - data concerning a person's sex life or sexual orientation
- Data relating to criminal convictions is treated separately and subject to even stricter controls

The following guidance is based on information we have gathered and training we have attended. It will be developed so please do let us have your input and feedback.

**If you collect email addresses from supporters:**

- Ensure data is stored securely eg. in a locked cabinet if you have paper records or under password protection if your data is stored online
- You don't need to write out to everyone on your mailing list if:
    - you have their consent to be on your mailing list
    - **or** if you have a 'legitimate interest' in contacting them and it is not against their interests / rights and they have the option to opt-out at any point - eg. if someone has attended an event you have organised in the past, you have a 'legitimate interest' to contact them with information that may be of interest to them ie. your newsletter or information about your group, providing they can opt-out at any point
- If your communication could be considered as 'direct marketing' (which includes campaigning or asking supporters to do something) rather than just information, you need their explicit consent to be on your mailing list.
- Whenever you collect addresses, make sure you have a privacy notice available (template at the end of this sheet) and a clear opt-in checkbox so that people are clearly consenting to be on your list. Keep that sheet as evidence of that consent (securely)
- Make sure any mail-out to your list has an 'opt-out' option. A service such as MailChimp will automatically include this and people can 'unsubscribe' themselves. If you do not use an automated service, think about how people will know they can opt-out and what your process is for removing someone's data if they request this.

**If you take and store photos:**

- If you take photos at an event, make it clear at the beginning that you will be doing so and give a clear option for opting out of photos eg. a 'no photos' sticker that someone could put on their shirt. Ask that anyone else taking photos also respects that some people may not want to have their photo taken.
- If you have a sign-in sheet at your event, have your privacy notice available and include a clear checkbox for photo consent. Keep that sheet as evidence of that consent (securely).
- For children, you will need a signed consent form from a parent or guardian before storing photos. Keep this consent form securely.
- You should only use pictures where you have explicit consent from the person depicted for you to use that photo for that purpose eg. if they agree for you to use the photo for 'general publicity' for your group, you could use it on your website or leaflets but couldn't pass it on to another organisation for them to use on their materials.
- If you are unsure if you have consent - don't use that photo.
- Delete any pictures that include someone who has not given consent to have their picture stored.

**If you collect personal data about volunteers or staff:**

- Ensure data is stored securely eg. in a locked cabinet if you have paper records or under password protection if your data is stored online.

- For volunteers, it is recommended that you have a Volunteer Agreement which they sign before they start. You may be able to get advice about this from your local CVS or Volunteer Centre. The agreement should include consent to store their data.
- Make sure you have a policy about how long you will store data after someone has finished volunteering or working for you and include this as part of the agreement that the person signs eg. as part of the volunteer agreement.
- If it is necessary for you to collect sensitive personal data (see p.1), we recommend that you seek specialist guidance to ensure you comply with the GDPR.

**If you collect personal data about sanctuary seekers / service users:**

- Ensure data is stored securely eg. in a locked cabinet if you have paper records or under password protection if your data is stored online.
- Make sure data is only accessible by authorised people and that everyone with access has a full understanding of your confidentiality policy and their responsibilities regarding data protection.
- You should have some way to record consent from someone to store their data eg. a consent form.
- Make sure you have a policy about how long you will store data and include this as part of any consent form that you use.
- If it is necessary for you to collect sensitive personal data (see p.1), we recommend that you seek specialist guidance to ensure you comply with the GDPR.

## Principles of the GDPR:

1. Personal data shall be processed **fairly and lawfully**
2. Personal data shall be obtained only for **specified and lawful purposes**
3. Personal data shall be **adequate**, relevant and not excessive
4. Personal data shall be **accurate** and, where necessary, kept up to date
5. Personal data processed for any purpose shall **not be kept for longer than is necessary** for that purpose
6. Personal data shall be processed in accordance with the **rights** of data subjects under this Act.
7. **Appropriate technical and organisational measures** shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall **not be transferred** to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

**Under the regulation, you need to have a reason to process personal data. Possible lawful reasons are:**

- You have explicit **consent** from that person to use their data for a specific purpose which you can prove
- There is a contractual agreement eg. you need a member of staff's bank details in order to be able to pay them

- You have a legal obligation or it is in the vital interests of the individual
- It is in the **legitimate interest** of the data controller (you) and is not prejudicial to the individual and they have the option to opt-out at any point eg. sending someone information that would be useful to them

## Data Audit

You may wish to undertake the following actions (this is for your own purposes, we don't need to see it but you may want to show it to your local CVS or Volunteer Centre):

1. Identify what personal data your group holds eg. email addresses of supporters, photos from events etc
2. Think about what data you will be collecting in the future and the reason for doing so and make sure it falls into the above categories
3. You may want to undertake a data protection assessment (see template)
4. It is recommended that you put together a Data Protection policy for your group (see template) and ask your local CVS or Volunteer Centre for advice on your draft version
5. You should use a privacy notice whenever you collect data in the future (see template)
6. Check if you need to register with the ICO - https://ico.org.uk/for-organisations/register/self-assessment/

## Useful Links

We will be updating our website with useful information about the GDPR:
https://cityofsanctuary.org/resources-for-groups/policies/

See also:

https://knowhownonprofit.org/organisation/operations/dataprotection

https://ico.org.uk/for-organisations/guide-to-data-protection/

**Privacy Notice Template**

This should be available where you are asking people to provide their personal data eg. at an event you could have a copy of your privacy notice next to your sign up sheet but be sure to include something on the sign up sheet that enables explicit consent eg. ☐ Please sign me up to receive your email newsletter plus any important updates via email.

We recommend that if your group needs to collect sensitive personal data, you seek specialist advice before putting together your privacy notice.

**Your Personal Data**

**What we need**

Your group name will be what's known as the 'controller' of the personal data you provide to us. We only collect basic personal data about you which does not include any special types of information or location based information. This does however include name, address, email etc

**Why we need it**

We need to know your basic personal data in order to provide you with information via our newsletter plus any important updates via email. We will not collect any personal data from you that we not not need.

**What we do with it**

All the personal data we process is processed by our staff in the UK. However, for the purposes of IT hosting and maintenance, this information is located on servers within the European Union. No third parties have access to your personal data unless the law allows them to do so.

We have a Data Protection regime in place to oversee the effective and secure processing of your personal data. Please contact us for more information about this framework.

**How long we keep it**

The information we use for marketing purposes will be kept until you notify us that you no longer wish to receive this information. Please contact us for more information about our retention schedule.

**What are your rights?**

If at any point you believe the information we process on you is incorrect, you can request to see this information and have it corrected or deleted. If you wish to raise a complaint on how have handled your personal data, please contact us. If you are not satisfied with our response or believe we are processing your personal data not in accordance with the law, you can complain to the Information Commissioner's Office (ICO).

**Contact details of your group**

**Data Protection Assessment**

This is optional - it may be useful to help your group think through how you collect and store data

(adapted from Community Matters template)

| |
|---|
| 1. Think about the types of personal data you process (eg. supporters' names and email addresses) and explain the justification for processing this data.<br>Include if you need to process sensitive personal data. |
| |
| 2. Think about the relevant legal basis relied upon to process personal data. If you are relying upon consent, please describe the method for obtaining consent (see section on reasons for processing data) |
| |
| 3. Think about the process by which you collect, use and delete personal data. You may want to create a flow diagram. |
| |
| 4. Identify privacy and related risks |
| |
| 5. Think about solutions and precautionary actions to minimise risks |
| |

**Template Data Protection Policy**

(adapted from the NCVO website)

Adapt for your group and ask your local CVS or Volunteer Centre for advice on your draft version (check / change the bits highlighted in yellow and fill in the empty boxes)

| **Who does the policy apply to?** |
| --- |
| This policy applies to..... |
| **Be familiar with the eight data protection principles specified in the GDPR and include these in your policy** |
| We will work in compliance with the principles of the GDPR:<br>1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –<br>(a) at least one of the conditions in Schedule 2 is met, and<br>(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.<br>2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.<br>3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.<br>4. Personal data shall be accurate and, where necessary, kept up to date.<br>5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.<br>6. Personal data shall be processed in accordance with the rights of data subjects under this Act.<br>7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.<br>8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data |
| **<u>Responsibility</u>**<br>**Allocate responsibility for GDPR compliance to a designated individual** |
| The named individual with responsibility for GDPR compliance in our group is... |
| **<u>Personal Data</u>**<br>**Explain what you mean by personal data and provide examples of the personal data that you may collect.**<br>**State the conditions for processing data (both ordinary and sensitive) and how you will identify and document the lawful basis for processing data (the lawful basis is the reason it is lawful for you to have that information ie. one of the reasons from the factsheet)** |
| Our definition of personal data is as follows... |

We will collect the following types of personal data...
The lawful basis for processing this data is...
In the future, we will establish the lawful basis for processing data by...
We will document this by...

**Compliance**

**Explain how your group demonstrates compliance with the GDPR - how you record the personal data processed, why it is being processed, categories of data, retention schedules etc.**

**The right to be forgotten**

**The right to be forgotten enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.**

We will respect the right to be forgotten - any individual can request for their personal data to be removed where there is no compelling reason for its continued processing.

**Retention of data**

**Outline what data is destroyed and when. Allocate someone to do this if possible.**

The different types of data that we have outlined above will be destroyed according to the following guidelines:...

- Financial records will be kept for seven years
-

**Access to data**

**Individuals have the right to request information that you hold about them. This is free of charge and you have one month to comply.**

Individuals have the right to request information we hold on them. There will not be a charge for this and we will comply within one month.

**Storage and security**

**Outline how data will be stored, who will have access to the data, what steps will be taken to ensure there is no unauthorised access and how data will be protected if it is taken off site.**
**Outline what your process is if there is a breach of security**