General Data Protection Regulation (GDPR)

Guidance for all volunteers

This guidance is intended for all Shared Interest volunteers. It explains what the General Data Protection Regulation (GDPR) is, why it is important, and what volunteers must do to comply with our legal obligations.

The guidance is divided into sections to help you navigate to your role or activity and find out what you need to do.

Shared Interest volunteers undertake many different activities, and we may not have covered every scenario. The GDPR is new for everyone, and we expect our guidance will evolve and improve over time, based on conversations with you and drawing on best practice guidelines.

The GDPR is an important and technical piece of legislation - and as a result, this guidance is necessarily very detailed and quite complex in areas. In some cases, volunteers may need to adjust how they run their activities, or even do additional tasks. However, as the GDPR is essentially about strengthening previous data protection legislation, this should not be completely new.

Please remember that the staff team is on hand to provide further guidance and support should you need it.

If you have any questions, concerns or want to talk through a particular issue, please contact the Volunteer Engagement Manager – sally.seddon@Shared Interest.org.uk or 0191 233 9100.

Contents

1. General Data Protection Regulation (GDPR)

1.1 What is GDPR?

General Data Protection Regulation (GDPR) is a new EU legal framework, which came into force on 25 May 2018. Its purpose is to give individuals more control and protection of their personal data. It introduces new regulations for all organisations that process (collect, manage and use) personal data. As Shared Interest processes data, and our volunteers process data on our behalf, we are legally required to comply with the GDPR.

The GDPR outlines the conditions under which data can be processed. These principles are similar to the 1988 Data Protection Act, but more specific. For example, people have to opt-into rather than opt-out of communications. This means there are additional requirements that we now need to follow when we collect, manage and use data.

The new accountability principle means there is now greater responsibility on organisations to document how they process and manage personal data. As volunteers process data on behalf of the Shared Interest, staff and volunteers need to work together to follow GDPR guidelines to make sure personal data is managed appropriately. Failing to do this may result in the Shared Interest being fined. We expect all of our volunteers to comply with the GDPR and these guidelines.

1.2 The six principles of the GDPR are:

1. **Lawfulness, fairness and transparency**: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
   The key thing here is consent - if you collect personal data you must clearly state why it is being collected, how it will be used, and you must record if consent was given. Similarly, when you are using people's personal data you must ensure you do so fairly, for example respecting their preferences.

2. **Purpose limitation**: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
   You may only collect personal data if you have a clear purpose for doing so, and you must not use the data for anything other than the purpose you have stated. For example, if you obtain an individual's contact details for the purpose of arranging an event, you may not contact them for any other purpose.

3. **Data minimisation**: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
   You must not collect more personal data than you need. For example, if you are arranging an event, you might just need name and contact details. Do not collect further data "just in case", like date of birth or gender.

4. **Accuracy**: Personal data shall be accurate and, where necessary, kept up to date.
   Will you be using this data on an ongoing basis? If so, how will you keep it accurate? If someone asks to be removed, you should do so, as soon as possible.
5. **Storage limitation**: Personal data shall be kept for no longer than is necessary for the purposes for which the personal data are processed.

Data should not be kept longer than needed. For example if the key contact of a fair trade group changes then you should delete the old contact information.

6. **Integrity and confidentiality**: Personal data shall be 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.

   You must be careful when managing personal data. For example, do not access personal data on a shared computer in a public library; do not store personal data on more devices than necessary; do not leave printed copies lying around. Do keep your personal devices as secure as possible.

If you are unsure about how you should be managing personal data as part of your role please contact the Volunteer Engagement Manager sally.seddon@shared-interest.com.

1.3 What data and activities does the GDPR apply to?

❖ **Personal data**

The GDPR outlines how personal data can be used. Personal data means any information relating to a living person who can be directly or indirectly identified by that information.

Personal data includes:

- Name (title, first name and surname)
- Postal address (full or partial e.g. postcode)
- Email address
- Telephone number (home or mobile)
- Membership number
- Online identifiers (such as IP address)

• Special categories of personal data

The GDPR also governs the use of sensitive personal data, which is now described as special categories of personal data - and there are stricter controls regulating the collection and use of this information. Sensitive personal data includes ethnicity, race, political affiliation, religion, union membership, health, sexual orientation etc.

Volunteers should not be handling special categories or sensitive data, so should not need to be familiar with these stricter controls.

❖ **Data processing**

The GDPR, like the Data Protection Act, is about how personal data can be processed. Data processing means:

- ✓ Collecting data
- ✓ Recording and holding data (electronically or in paper-based filing systems)

- ✓ Any activity that uses the personal data (such as organising, adapting, changing, retrieving, consulting, disclosing, erasing or destroying the data).

For example, you are processing data when contacting other volunteers to send out information about an event or asking for help with an event

As volunteers, you have been following our previous data protection guidance, so although there are some new requirements brought in by the GDPR, it is mainly about enhancing what you are already doing.

1.4. How the GDPR applies to volunteers - who is responsible?

One of the key changes with the GDPR is the accountability principle, which places greater responsibility on organisations to clearly explain and document why data is being collected and how it is being used.

Shared Interest volunteers are not data controllers, and therefore cannot decide the purposes for processing data, and must comply with the Shared Interest policies and guidelines.

If you are handling data in any way, please get in touch with the Volunteer Engagement Manager to discuss how to proceed.

Data protection is everybody's responsibility. As a Shared Interest volunteer, you may process data on behalf of the Shared Interest. If so, you are responsible for looking after other people's data.

All volunteers must be aware of and understand the 6 principles of the GDPR to ensure that any processing of personal data you undertake as part of your volunteering duties is carried out correctly.

If you stop performing a volunteer role, you should inform the Volunteer Engagement Manager of any data you have been managing and agree if this should be destroyed, returned to Shared Interest or handed over to another volunteer. You must not retain any copies of personal data.

2. How the GDPR applies to different types of data

2.1. Membership data

Shared Interest collects members' data for the purposes of servicing their Share Account, and we can contact members in relation to their investment, regardless of their contact permissions. For example, to issue a statement or send out AGM papers.

However, if we want to contact members about anything, which is not directly related to their investment - we can only do so if we have their consent to contact them.

We collect contact preferences and consent for non-member related communications at the point of enquiring, and members can manage their contact preferences through the member portal or by contacting us directly. Details and options for unsubscribing from communications are also included in all e-communications. Enquirers can opt in or out of further communication from us, using the tick box on the insert or online enquiry form.

The Shared Interest membership and volunteer databases contains all personal data, contact preferences for members', enquirers and volunteers.

To ensure we follow these preferences please do not contact members directly.

2.2. Non-member data

If you collect personal data, you are responsible for ensuring it is collected, managed and maintained in accordance with the GDPR. We therefore recommend that volunteers refrain from collecting personal data where possible.

If you are collecting personal data from groups or clubs, you must obtain consent, record how and when you obtained consent, and document how you are managing the data. To do this, please follow these steps:

1. Remind yourself of the key principles of the GDPR
2. Speak to the Volunteer Engagement Manager on how to apply the GDPR in your role.
3. Use a clear statement of consent

> "Any freely given, specific, informed and **unambiguous** indication of the person's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

4. You must be transparent, informative and clear about why you are collecting data and how it will be used. (See the data mapping template in the GDPR toolkit to record the process)
5. Have a positive opt-in
6. Consent must be informed and freely given.

> You cannot assume consent or use "opt-out, pre-ticked" boxes - people must take action and choose to give you consent.

7. Document when and how consent was obtained and provide a copy to Shared Interest
8. You must be able to demonstrate that consent has been given. This could be by making a note on the data list, or by securely keeping consent forms.

9. Ensure that data is stored securely and do not keep it longer than needed
10. Document your process in writing

NB: If you are handling non-member data e.g. contact details for a local fair trade group or Rotary Club, please contact the Volunteer Engagement Manager sally.seddon@Shared-interest.com to ensure you are compliant with GDPR.

2.3. Children's data (anyone under 16)

The GDPR has very strict rules around how children's data must be managed. A person over the age of 16 can open a Share Account but anyone younger cannot. Under 16's can, however, be named on a Share Account with the parent or guardian's details stored in our membership database. Although we do not directly work with children you may be involved in school presentations and could meet children at events.

Shared Interest's safeguarding policy states that volunteers should, wherever possible, be accompanied by a second adult when their activity involves children.

When taking photos, please ensure no individuals under 18 are photographed without explicit consent from their parent or guardian (for more details please see section 3.4).

2.4. Photographs

Photographs of people are a type of personal data and in some cases, you may need to collect consent from the people you are photographing. Guidelines differ depending on the purpose of the photograph, how many people are in it and, if individuals are identified. Particular care needs to be taken if children are present.

Please see section 3.4 for more details.

3. All volunteers: how the GDPR applies to volunteer activities

Shared Interest's volunteers carry out a wide range of activities on behalf of the organisation.

Volunteers must not create and keep locally sourced data or lists of members/supporters and their details. It is important that there is one set of authoritative data, held and processed centrally by Shared Interest, otherwise it creates a confusing situation and makes it hard for Shared Interest to be GDPR compliant.

Members tell Shared Interest if and how they want to be contacted - whether by email, phone or post. Contact preferences apply to all communications that are not core to fulfilling membership contracts.

All, and any, contact with members will be done by Shared Interest and volunteers should not be contacting members directly.

3.1 Bulk emails

Volunteers do not currently use a bulk-mailing tool to communicate.

However, if you are using email systems like Outlook or Gmail which are designed primarily for emailing small groups of people, please remember it's essential that you:

- ✓ Use the bcc field, not the cc field, to avoid exposing everyone's email addresses.
- ✓ Include text at the bottom explaining how people can be removed from your distribution list (e.g. by emailing you back and requesting you to update their preferences).

3.2 Collecting speaking or event contacts

Many of the organisers of events will use their personal information for contact purposes. If you collect personal data, you are responsible for ensuring it is collected, managed and maintained in accordance with the GDPR.

If you collect personal data, you must obtain consent, record how and when you obtained consent, and document how you are managing the data.

When communicating with contacts it is essential that you:

- ✓ Can demonstrate their informed consent to contact them by using the example consent form provided by Shared Interest.
- ✓ Provide an opt-out.
- ✓ Respect their preferences if they choose to opt-out.

3.3 Working with other volunteers

Volunteers will often hold personal contact details of other volunteers to enable them to coordinate Shared Interest activities locally. For example, an event with a number of volunteers helping on a stall.

All volunteers are responsible for ensuring they keep personal contact details secure and up-to-date (for example, removing individuals if they stop volunteering). Contact lists should be destroyed as soon as they are out of date or no longer needed.

3.4 Taking and publishing photographs

Photographs of people are a type of personal data. However, there is not yet detailed guidance about how the GDPR applies to photos. Nevertheless, you should always seek consent before taking or publishing photos. We recommend that in the case of:

- Staged photos of a group where you gather a group of people together to take a photo.

You must inform the group if the photo will be published and where (for example, our website, social media, a newsletter) and confirm people are willing to be photographed for that purpose.

- Candid photos of a group taken when people were not aware and are not easily identifiable.

If this photo is intended for commercial or marketing use (for example, on a printed leaflet), or it will be used to identify individuals by name, you will need to be able to demonstrate their consent. The easiest way to do this is by completing a written photo consent form, available in our GDPR toolkit.

However, if you are simply showcasing the activity on a website, social media, newsletter (online or print), and you do not identify people by name or share other personal data, you do not need their written consent.

- Photos of one or two people where the individuals are the main focus of the photo and identifiable

You must inform the person/people if the photo will be published and where (for example, our website, social media, a newsletter) and confirm they are willing to be photographed for that purpose.

If it is intended that the photo is to be published in any way (for example, website, newsletter, social media or printed materials), you will need to be able to demonstrate their consent. The easiest way to do this is by completing a written photo consent form.

- Photos of children

You must not take photos of children unless their parent or legal guardian has given explicit permission. If it is intended to publish the photo in any way (for example, website, newsletter, social media or printed materials), you also need to have the consent of their parent or legal guardian. The easiest way to do this is by completing a written photo consent form.

NB. We will update this guidance and associated consent forms as further information becomes available. Please look out for further communications.

4. All volunteers: how to apply the GDPR in your role

Data protection is everybody's responsibility. As a Shared Interest volunteer, you may on occasion, process data on behalf of the Shared Interest. If so, you are responsible for looking after other people's data.

You must also be aware of and understand the 6 principles of the GDPR so that if you need to process personal data as part of your volunteering duties, you know how to do so safely and legally. Not all principles will apply to every situation, but they will help you handle data carefully and appropriately.

If you are unsure about how you should be managing personal data as part of your role please contact the Volunteer Engagement Manager, sally.seddon@shared-interest.com.

5. Subject access requests

Under the GDPR, individuals can request to see their data. This is called a "subject access request". If you receive one of these, please do not respond, but notify the Volunteer Engagement Manager (sally.seddon@shared-interest.com) within 24 hours who will advise on next steps.

6. Keeping data safe and secure

6.1 Electronic data.

Keeping your personal devices secure is one of the best ways to safeguard personal data stored electronically. Here are some simple things to keep your electronic devices, and all the data on them, safe:

- ✓ Establish strong passwords and/or passcodes for all your electronic devices (laptops, personal computers, tablets and smartphones). Where possible, make sure you use a combination of letters and numbers for a hard-to-crack password.

- ✓ Keep laptops secure by using a username and a unique password. Make sure to never leave your laptop or any device where it is at the risk of being stolen or compromised, for example in a car.

- ✓ Use antivirus protection and anti-malware software. These serve as the last line of defence against unwanted attack through your network.

- ✓ Update your computer programmes regularly. Data security is enhanced with every update. Frequently updating your programs keeps you up-to-date on any recent issues or holes that manufacturers and programmers have fixed.

- ✓ Enable your device to lock after a short period of time. Most devices do this automatically, so after a set time devices "lock". This is useful so that your devices are protected if you have to leave your screen for any period.

- ✓ Avoid using public PCs or laptops for official use as in most cases you are unable to verify the level of anti-virus or online security on the devices.

In this case, make sure all physical copies are kept carefully and securely to avoid them being been seen or used by unauthorised people, stolen, tampered with or used for alternative purposes by any third party. To do this, keep data together in a file and ideally out of sight when

not in use - for example in a drawer. As soon as the data is no longer needed, securely destroy the data by shredding.

6.2 Paper documents

We recommend that you do not print out personal data or keep paper copies of data, as this is the least secure way to manage data. However, sometimes you may need to. In this case, make sure all physical copies are kept carefully and securely to avoid them being been seen or used by unauthorised people, stolen, tampered with or used for alternative purposes by any third party. To do this, keep data together in a file and ideally out of sight when not in use – for example in a drawer. As soon as the data is no longer needed, securely destroy the data by shredding.

7. Disposal of data

Storing and archiving data is considered 'processing' of personal data, even if the data is not used or updated. Therefore to comply with GDPR, personal data must be securely disposed of when it is no longer needed.

7.1 Electronic data

Electronic data must be completely deleted when it's no longer needed.

- ✓ If deleting data within a file, delete the data from the file, and then re-save the file. If deleting a whole file containing data, delete the file and then go to the Recycling Bin on your computer and delete the file from there too.

- ✓ Any CDs and/or DVDs containing personal data must be cut up or crushed before being thrown away.

- ✓ When disposing of old equipment (such as PCs), please be mindful of data security. Devices that don't have removable storage media, such as mobile phones, usually come with a function called something along the lines of 'Restore to factory settings' to wipe the data.

7.2 Paper documents

Paper documents should be shredded and put in the bin (not recycling) or disposed of using suitable confidential waste facilities.

8. Security breaches

A data security breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples

of data breaches include:

- Mobile devices, briefcases and bags stolen from vehicles.
- A website with personal data being hacked.
- Documents with personal data missing after being left unattended.
- Used computers or mobile devices sold without first destroying personal data.
- Lost, unencrypted memory sticks and drives containing sensitive information.

If a breach has occurred, or you are worried one might have, please notify Shared Interest within 24 hours who will advise on next steps.

9. Training and further support

We are aware that this is a complex area, and extra training and support may be useful. We will inform you of training opportunities and further guidance as it becomes available. Please look out for further communications.

If you need further help, have questions or concerns; please get in touch with the Volunteer Engagement Manager (sally.seddon@Shared Interest.com).