General Data Protection Regulation (GDPR)
Guidance for all Ramblers volunteers

Overview

This guidance is intended for all Ramblers volunteers but will be particularly relevant for membership secretaries who have an enhanced responsibility to manage members' personal data. It explains what the General Data Protection Regulation (GDPR) is, why it's 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.

Ramblers 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. Our General Data Protection Regulation (GDPR) toolkit includes all our resources and an FAQ which will be kept up to date, so please refer to this and look out for further communications.

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 work. However, as the GDPR is essentially about strengthening previous data protection legislation, this shouldn't all 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 Ramblers data protection officer - dataprotection@ramblers.zendesk.com or 0203 961 3232.

Contents

1 The General Data Protection Regulation (GDPR)

1.1 What is the General Data Protection Regulation (GDPR)?

The General Data Protection Regulation (GDPR) is a new EU legal framework which comes 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 the Ramblers process 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 Ramblers groups and areas process data on behalf of the Ramblers, 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 Ramblers being fined.

1.2 What data and activities does 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 eg. 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.

Area and group volunteers should not be handling special categories or sensitive data at a local level, so should not need to be familiar with these stricter controls . However, there may be some exceptions - for example, Incident Report forms which contain health data - which are addressed later in this guidance.

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).

Examples of data processing at a local group or area level are:

- Using the membership lists to send out your group or area's walk programme
- Filling in an Incident Report form
- Publishing a walks programme which includes walk leaders' names and contact details.

Your group and area will have been following our previous data protection guidance, so although there are some new requirements brought in by the GDPR, it's mainly about enhancing what you are already doing.

1.3 The principles of the GDPR

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.
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.
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.
4. Accuracy: Personal data shall be accurate and, where necessary, kept up to date.
5. Storage limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
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.

1.4 How the GDPR applies to volunteers – who's 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.

The Ramblers' data controller (the Head of ICT and Web services) is responsible for determining the purposes for processing data i.e. how and why data is processed.

Ramblers areas and groups are not data controllers, and therefore cannot decide the purposes for processing data, and must comply with the Ramblers national policies and guidelines.

Data protection is everybody's responsibility. As a Ramblers volunteer, you may process data on behalf of the Ramblers. 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 your area/group membership secretary of any data you have been managing and agree if this should be destroyed or handed over to another volunteer. You must not retain any copies of personal data.
Membership secretaries handle local membership data and so must be particularly aware of GDPR regulations. Please see section 4 for more details. Membership secretaries who are stepping down must have a handover process in place - please contact the dataprotection@ramblers.zendesk.com if you need further advice.
Chairs are responsible for the smooth running of their group or area and for ensuring they comply with the Ramblers' legal obligations and organisational policies. In relation to GDPR, they are responsible for ensuring volunteers in their group or area are aware of this GDPR guidance.

2 How the GDPR applies to different types of data

2.1 Membership data

The Ramblers collects members' data for the purposes of servicing their membership, and we can contact members in relation to their membership, regardless of their contact permissions. For example, to issue new membership cards or send renewal reminders.

However, if we want to contact members about anything which is not directly

related to fulfilling their membership contract – such as fundraising appeals - we can only do so if we have their consent to contact them.

We collect contact preferences and consent for non-membership related communications at the point of joining, and members can manage their contact preferences through their web account or by contacting us directly. Details and options for unsubscribing from communications are also included in all communications sent out by Ramblers' offices.

The Ramblers central database contains all members' personal data and contact preferences. Direct marketing contact preferences are included in the membership lists and reports sent to membership secretaries on a weekly and monthly basis.

Contact preferences apply to all communications from the Ramblers – including those sent by areas and groups. Please ensure you follow these contact preferences and – importantly – do not contact members who have opted out of communications. For more details about direct marketing and contacting members, please see section 5.2.

NB: To help ensure you are compliant with GDPR, *we strongly recommend* that you only use the reports and lists provided by Ramblers' offices to manage communications locally.

Creating local data sets and lists could create confusion and lead to a data breach.

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 areas and groups refrain from collecting personal data from non-members.

If your area or group is collecting personal data from non-members, 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:

- Remind yourself of the key principles of the GDPR See "How to apply the GDPR in your role" (section 6).
- Use a clear, unambiguous consent statement
    - You must be transparent, informative and clear about why you are collecting data and how it will be used.
- Have a positive opt-in
    - Consent must be informed and freely given. Therefore, you cannot assume consent or use "opt-out, pre-ticked" boxes – people must

take action and choose to give you consent.

- Document when and how consent was obtained
    - 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.
- Ensure that data is stored securely and do not keep it longer than needed Please see section 8 for guidance.

NB: If you are handling non-member data locally, please contact the dataprotection@ramblers.zendesk.com to ensure you are compliant with GDPR.

2.3 Children's data (anyone under 18)

The GDPR has very strict rules around how children's data must be managed. Because we do not regularly work with children, the Ramblers does not have the required safeguards in place. It is therefore our policy that we will not collect or process any data from under 18s.

Ramblers' safeguarding policy states that under 18s may only participate in Ramblers activities if accompanied by a responsible adult. Only the personal data of the adult should be collected, not the personal data of the child.

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 5.10).

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 5.10 for more details.

3 Chairs: your responsibilities

As chairs, you are responsible for the smooth running of your group or area, and for ensuring you comply with the Ramblers' legal obligations and organisational policies. This now includes ensuring your group or area are following this guidance and are compliant with the GDPR.

Raise awareness of data protection

Please make sure the volunteers in your group or area are aware of this guidance:

Quick guide to keeping data safe

4 Membership secretaries: your responsibilities

As membership secretaries, you receive regular lists and reports relating to members in your group or area. As you are personally handling sensitive data, you have enhanced responsibilities under the GDPR to manage data securely and safely. It is therefore particularly important that you are aware of good data protection.

4.1 Receiving and using membership data

When you receive membership lists and reports from Ramblers' offices, it is your responsibility to:

Manage access to the membership lists and reports

Only the membership secretary should have access to the membership reports and lists which are sent from Ramblers' offices. If other volunteers need to use membership data (for example, to send a group newsletter), the membership secretary must share only the relevant data to enable them to do so. For example, a communications volunteer sending an email newsletter does not need access to postal addresses.

Manage mailboxes securely

Membership secretaries must not use shared mailboxes – this is a high risk practice as it enables multiple people to access all membership data.

Securely store membership lists and reports if you need to hold them temporarily.

Only one membership report/list at a time should be kept and for as little time as possible. When you receive new reports and lists, the old reports and lists should be deleted. This will help ensure compliance with the GDPR principles of accuracy and storage limitation. New membership reports/lists will always have the latest and most accurate data. If you wish to track the size of your membership, please retain only the membership count. Personal data is not required for this.

Please see section 8 for more guidance on how to store data securely.

Ensure members' data is used appropriately and contact preferences are respected From May 2018, the membership lists and reports sent by Ramblers' offices will include members' contact preferences. You must abide by these contact preferences. For example, if a member has opted out of email and postal communications, you may not send them fundraising requests.

Contact preferences apply to all communications that are not core to fulfilling membership contracts. For example:

- Sending details of local campaigns
- Fundraising requests to donate to the Ramblers
- Recruiting volunteers

There may be circumstances when volunteers need to contact a sub-set of individuals because an activity they were involved with has changed or cancelled, for example a planned walk has been cancelled because of snow. Volunteers can contact these individuals, but if an individual requests not to be contacted in this way again, please make a note and respect this in the future.

The following activities are considered core to the fulfilment of membership contracts, and therefore contact preferences do not apply:

- Contacting new members to welcome them
- Sending information about activities your group or area is running, for example socials, walking festivals or events
- Sending annual reports
- Sending a one off reminder to existing members to renew their membership
- Sending AGM notices

The following activities are considered legitimate interest communications. In these cases, because of the way the law works, postal preferences don't apply but email preferences do:

- Sending newsletters
- Sending combined walk programmes/newsletters

For more guidance on walk programmes and newsletters, please see section 5.4

Ensure membership data is only shared with other volunteers to enable delivery of Ramblers activities

You are responsible for the sharing and use of personal data in your group or area. Therefore, if another volunteer asks for access to membership data, or wants to contact members directly, you must ensure it is a legitimate use of membership data. For example, sending out an AGM notice is legitimate, promoting a fundraising event by another local charity is not.

When sharing membership data with other volunteers, you must only share what is needed. You should also remind the volunteer that:

- they should be familiar with this guidance;
- they need to respect members' contact preferences;
- they should destroy the data as soon as their activity is complete.

Be an ambassador for good data protection and support other volunteers

Your role as a membership secretary means that you will likely know more about data protection than other local volunteers. As the primary data handler for your group or area, you may also be asked for data by other volunteers. You therefore have a responsibility to model and ensure good behaviour locally.

Wherever possible, remind fellow volunteers:

- of the importance of data protection;
- that if they are collecting or using any personal data they should consult and follow this guidance;

Volunteers may also ask you questions – please help as best you can, which will usually involve directing volunteers to this guidance. If you are unsure of the answer, please get in touch with our dataprotection@ramblers.zendesk.com.

4.2 Updating membership data

A key principle of the GDPR is that data must be accurate, so it's very important that the Ramblers' central database is the authoritative record of members' details.

Members' personal data should be updated by members updating their own record via the Ramblers' website, by contacting the membership services team.

This is important for enabling us to manage our data effectively, and ensures all data shared by Ramblers' offices is accurate and up-to-date.

The quickest and easiest way for members to update their information is by logging into their account on the Ramblers website and changing their details in "My account". http://www.ramblers.org.uk/my-account

If they do not have an account, they should be advised to create one. http://www.ramblers.org.uk/my-account

If they do not have access to the internet, they can call the membership services team on 0203 961 3232.

5 All volunteers: how the GDPR applies to common volunteer activities

Ramblers' volunteers carry out a wide range of activities on behalf of the organisation,which often involve managing individuals' personal data. Below are some of the common activities, along with an overview of what you need to do to ensure you're compliant with the GDPR.

NB this is not a comprehensive list

5.1 Using membership reports and lists issued by Ramblers' offices

Membership secretaries normally access their lists through the Insight Hub. They

are therefore responsible for ensuring that data is collected, managed and used properly within the group or area.

Anyone wishing to contact members locally should liaise with their relevant membership secretary to ensure they have a legitimate reason for contact, and they are following the necessary guidance. Detailed information on accessing and using data to contact members and supporters locally is outlined in section 4.

Please remember that only reports from the Insight Hub should be used as your base membership data set. It is important that there is one set of authoritative data, otherwise it creates a confusing situation and makes it hard for the Ramblers to be GDPR compliant.

5.2 Contacting members

Members tell the Ramblers 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. You must abide by these contact preferences. For example, if a member has opted out of email and postal communications, you may not send them information about local campaigns by email or post.

Group and area membership secretaries are responsible for ensuring any volunteers wishing to communicate with members locally have access to up-to-date data lists and are respecting contact preferences. Please see section 4 for more details.

If you are contacting members, please remember:

- You must use the most recent membership data supplied by Ramblers' offices to the group or area membership secretary to ensure data is accurate.
- You must not contact members who have opted-out. Data lists should not be retained past the purpose for which they were obtained.

Managing opt-outs and unsubscribes locally

You must include a clear opt-out option or unsubscribe message in all email or postal communications.

To avoid confusion and ensure that local and national records are consistent, we recommend members are encouraged to update their central record. The following message must be included in all email or postal communications aside from the examples detailed below:

> *'You are receiving this communication as a member of X area/group and you have previously asked to be kept informed of the Ramblers work (including local walks, local footpath protection,*

access campaigns, fundraising & volunteering). If you no longer wish to receive communications by email/or post, please update your mailing preferences here '

If your group or area is using a bulk mailing tool to communicate, you may find there are built in safeguards to improve security. This might mean emails automatically include an unsubscribe link. This could result in people opting out of communications locally, whilst still remaining opted-in on the central database.

To help us manage our data and avoid breaches, we therefore require you to contact Ramblers' offices with any unsubscribe information you collect, so we can update our central records. More detailed guidance on managing data in bulk mailing tools is available in the GDPR toolkit.

There may be instances where a member is not receiving your communications. If so, let them know that you communicate with those who are opted into Ramblers communications and advise them to update their contact preferences via the Ramblers website or by contacting the membership services team.

There may be instances when a member's record shows they are opted-in to receive communications, but they have directly told you they do not want a particular communication. In this case please advise them to update their central membership record online or by getting in touch with the membership services team, reminding them that this will opt them out of all Ramblers communications. (See section 4.2 on how members can do this).

Sending bulk emails locally

We do not currently require volunteers to use a standard tool for email locally, and we know that different areas and groups use different systems. However, we do encourage volunteers to use bulk email tools (for example, MailChimp) as they have safeguards built in to help improve data security. The Ramblers use MailChimp centrally, and we will be adding specific guidance to the GDPR toolkit to help you manage mailing lists effectively in MailChimp.

However, if you are using email systems like Outlook or Gmail which are designed primarily for emailing small groups of peoples, 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 the mailing list (eg by emailing you and updating their preferences on the Ramblers website).

5.3 Contacting non-members

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 areas and groups refrain from collecting personal data from non-members.

If your area or group is collecting personal data from non-members, you must obtain consent, record how and when you obtained consent, and document how you are managing the data. Please see section 2.2 for more details.

When communicating with non-members, it is essential that you:

- Can demonstrate their informed consent to contact them.
- Provide an opt-out.
- Respect their preferences if they choose to opt-out.

We strongly recommend that you don't have mailing lists which are a mix of members and non-members. But if you do, please ensure you have consent to contact non- members, and that you abide by members' contact preferences as shown on the lists sent by Ramblers' offices.

5.4 Sending newsletters

Newsletters are considered legitimate interest communications. However, different law applies depending whether you send them by email or by post. This means newsletters can be sent by post to members regardless of their contact preferences. However, when sending a newsletter by email, you must abide by contact preferences and only email it to individuals who have opted-in to email communications from the Ramblers– this will be shown on the Insight Hub. If a member asks not to receive a printed newsletter by post, you must make a note of this and remove them from the distribution list.

5.5 Working with other volunteers

Volunteers will often hold personal contact details of other volunteers to enable them to coordinate Ramblers activities locally. For example, a walks programme coordinator may have a list of walk leaders, or a path maintenance team leader may have a list of volunteers in their parish. 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.

5.6 Volunteer recruitment

Only members who have given consent to receive communications from the Ramblers should be contacted with information about volunteering opportunities in your area or group.

5.7 Publishing volunteer contact details

You must not share volunteer contact details on any channel – for example in walk programmes or on the Group Walks and Event Manager – unless you have their consent to do so. Before publishing any volunteer contact details, please ask

them to complete a "Publishing volunteer details" form. You only need to do this once, but please keep a copy of the form securely (see section 8 for more advice). You may also want to keep an easy record of who has given consent and when, for example a note alongside your list of walk leaders.

5.8 Taking walk registers

If you are taking walk registers, we recommend you use the walk register provided in the walk leader toolkit, which has appropriate GDPR statements on it.

You must not collect walkers' health information or the personal data of their emergency contacts on walk registers. Please order In Case of Emergency cards from Ramblers' offices for this purpose.

If you are collecting non-members' contact details (for example email addresses so you can tell them more about your group and the Ramblers) please follow the guidance in section 2.2.

You must not retain walk registers *with personal data on them* - please destroy them one month after the walk.

5.9 Reporting incidents on walks

If there is an incident on your walk, please complete our Incident Report form and return it within 10 days. Please use the latest version, found in the walk leader toolkit, and do not keep any copies locally.

5.10 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 (for example, after completing a path maintenance activity, or at the top of a hill during a group walk)

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

If you wish to use this photo for commercial or marketing purposes (for example, on a printed leaflet), or 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.

However, if you are simply showcasing your group/area's activity on your group/area's website, social media, newsletter (online or print), and you don't identify people by name or share other personal data, you do not need their

written consent.

Candid photos of a group taken when people weren't aware and aren't easily identifiable (for example, a group walking along the coast in the distance).

If you wish to use this photo for commercial or marketing purposes (for example, on a printed leaflet), or 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.

However, if you are simply showcasing your group/area's activity on your group/area's website, social media, newsletter (online or print), and you don't 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/or easily identifiable

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

If you wish to publish the photo in any way (for example, your 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 you wish to publish the photo in any way (for example, your 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.

If you need to collect written consent, please use the "Media consent form" in the GDPR toolkit.

5.11 Websites

If you manage a website for your area or group, you must include a link to our privacy policy

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 areas and groups refrain from collecting personal data locally. If you collect personal details through your website (for example, through a login so only members can see some content, or a newsletter sign up), follow the

guidelines in section 2.2 to ensure informed, opt-in consent.

If you have any specific concerns or questions, please email dataprotection@ramblers.zendesk.com

Booking holidays and coach trips

When you start to organise a holiday, consider what data will be required (only collect the minimum), and confirm if any third parties will require people's data (for example, a travel company). When you collect data you must inform people how it will be used and ensure you have consent for it to be passed on as required. For example: "I am collecting your name, postal address and email and will be passing it to [name of company] so that they can book this holiday. Please confirm that you are happy for me to pass on your details. If you have any questions, please get in touch with [volunteer name]".

You must not retain this data – it should be destroyed no later than one month after the holiday.

5.12 Booking training and events

If you are using a third party website, such as Eventbrite to book training and events, this will generate lists of personal data (eg. email address, name). You may use this data for the purposes of administering the event. The event and all associated data must be deleted once the event has passed and it is no longer needed. Data may not be extracted for any other purpose or use not directly related to the event.

5.13 Publishing committee/AGM minutes

There are a few ways of reporting minutes of meetings on your website or on your online platforms. Volunteers may give consent for their names to be published online publicly or on a password protected file only accessible to members. You may also decide to redact (remove) the names of the officials or use their role titles within the group for anonymity. The right option will depend on what is decided within your group. Just ensure no names or personal details are published without the necessary consent.

5.14 Historical collections of data

If your group has historical collections of data, please contact dataprotection@ramblers.zendesk.com to discuss how best to manage it.

6 All volunteers: how to apply GDPR in your role

Data protection is everybody's responsibility. As a Ramblers volunteer, you may process data on behalf of the Ramblers. 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.

The 6 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're using people's personal data you must ensure you do so fairly, for example respecting mailings 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 may 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 a holiday they are coming on, you may not add them to your local newsletter mailing list.

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're arranging a holiday, you might just need name and contact details. Do not collect further data "just in case", like date of birth or gender, if you don't need it for your purpose.

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? For example, if you're a path team leader and maintain a list of path team volunteers, it would be good to check every 6 months that people still want to be on the list and their details are correct. And if someone asks to be removed, you should do that as soon as possible.

5. **Storage limitation**: Personal data shall be 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.
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 (see section 8 for more guidance).

If you are unsure about how you should be managing personal data as part of your role, please contact dataprotection@ramblers.zendesk.com

7 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 dataprotection@ramblers.zendesk.com within 24 hours who will advise on next steps.

8 Keeping data safe and secure

8.1 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 remember 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.

8.2 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.

9 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.

9.1 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. Some retailers, such as the larger Currys PC World stores, offer a secure data wiping service for around £35. For those without access to a high street store there is software available online that will overwrite the entire hard drive to remove the data – see https://dban.org/. 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.

9.2 Paper documents

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

10 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.

The failure to report a data breach quickly is now viewed as seriously as the breach itself by the Information Commissioner's Office. So we may well not get a fine for a data breach but not reporting it is viewed as covering it up. That same €20m fine applies if we don't report any breach within 72 hours. So always report anything as soon as you even suspect something may have gone wrong. We'll then help you work out what happened, what we need to do next and will be able to complete any relevant reporting to the ICO.

Just email details of what's happened to dataprotection@ramblers.zendesk.com giving your name and a phone number where we can contact you.

11 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 and it becomes available. Please look out for further communications.

In the meantime, you can:

- Look through our FAQ in the GDPR toolkit which we are regularly updating.
- See if there is a Ramblers Roadshow happening near you and come along to a GDPR workshop.

If you need further help, have questions or concerns, please get in touch with the Ramblers data protection officer dataprotection@ramblers.zendesk.com or 0203 961 3232.