Data protection under the GDPR: Frequently asked questions

About this document 1
About the GDPR 2
What does the GDPR mean for us? 3
Filing and data retention 3
Personal data breaches 5
People who aren't members 6
Members: Data storage and data sharing 7
IT (email use and storage) 8
Group Handbook A6: Handling data 9
Guidance, policies and Data Protection Essentials online learning 10
Newsletters 11
Passwords and security 12
Third parties 14
Glossary of GDPR terms 15

About this document

This document includes frequently asked questions (FAQs) and answers regarding the GDPR, and is for anyone in an MS Society volunteer-led group who handles people's data.

Where this document refers to 'we', unless otherwise stated, we mean staff and volunteers. Where we use the word 'must' or 'we expect you to', it means a specific rule that you must comply with. Where we use the words 'we want you to' or 'we recommend', these indicate our suggested best approach.

You can click on any text that is underlined and coloured in blue to take you to the further information mentioned.

This FAQ was created on 23 March 2018 and is the first edition.

Sources of support

If you have a question that isn't answered here, please contact the Data Governance Team by email at datagovernance@mssociety.org.uk.

You can also speak to your Local Networks Officer (LNO). See Local Networks Team on our volunteer website for contact details for your LNO.

For a quick guide to the GDPR see our Six Tips: Question it, learn it, log it, lock it, secure it, tidy it. Please share these tips with those who volunteer alongside you.

About the GDPR

1. What is the GDPR?

The General Data Protection Regulation (the GDPR) is the new law for data protection. On 25 May 2018 it will come into force, replacing the Data Protection Act (1998). It is based upon the same principles as the current Data Protection Act, but introduces new rights for individuals, and increases the obligations of organisations that handle data about people.

2. What is data?

'Data' or 'personal information' means a piece or pieces of information which can identify a living person. This personal data includes name, email, address, date of birth, and interests.

Sensitive personal data or 'special characteristics' such as health information, sexuality and religious beliefs are given even more protection under the GDPR.

3. What is data protection?

Protecting data according to the law means:

- We respect the privacy of people's personal information.
- Our volunteers, members and other contacts know how we look after their personal information.
- We are able to respond to people exercising their rights, such as opting in or out of receiving messages from us, or objecting to their data being processed at all.

4. What is data processing?

Data processing includes anything we do to, or with, personal information, such as filing, updating, copying, checking or sharing. Data processing also covers simply storing data even if nothing is done with it.

What does the GDPR mean for us?

5. Does the GDPR change my role as a group volunteer?

The GDPR introduces some specific new requirements that you need to know about. If you handle personal data, we will support you to learn about these by:

- For some roles, completing our Data Protection Essentials online learning to learn about the law. Training updates will be included in Teamspirit or you can ask your LNO.
- Reading our guidance on handling data on the volunteer website.
- Referring to these FAQs when you are handling or processing data.
- Making sure all volunteers in your group are up to date with how they should be processing or handling data.

The GDPR requires that we make sure to protect the privacy rights of all people whose personal data we have access to, or proactively gather. This may mean you need to change some of the ways you carry out your role. However, your role description remains the same.

Filing and data retention

6. Apart from newsletters (see question 30), how long can we keep other information gathered such as membership lists, thank you letters and cards?

Membership lists should not be retained beyond the individual task at hand, but downloaded from the Portal each time you need to contact people.

Thank you letters and cards to individuals can be kept indefinitely by those individuals, but if they contain any sensitive personal information you must ensure that this is kept securely.

Groups must not use membership data that is more than 28 days old.

7. Is there a recommended time for keeping various pieces of information?

Yes – please refer to our data retention guidance in Group Handbook A6: Handling data.

To comply with our Health and Safety requirements, health and safety documents such as Physical Activity Readiness Questionnaires (PARQs) should be reviewed annually and destroyed if the person is no longer involved in the activity.

However, if you set up a service level agreement (SLA), PARQs and disclaimers will be the responsibility of your service provider, so you won't have to worry about keeping them. Speak to your LNO about setting up SLAs.

8. Are minutes of a meeting subject to the GDPR and how should we store them?

You should avoid recording any sensitive personal data in any notes taken of official meetings that will be distributed to Coordinating Team members. If it is necessary to minute a meeting where personal data is important, you need to ensure that these are password protected and held on an encrypted computer if electronic, or kept in locked storage if paper.

9. I handwrite notes for my own understanding of meetings and sometimes record telephone numbers, addresses etc., of individuals in my notepad. Are these handwritten notes in notepads subject to the GDPR?

Handwritten notes with personal information in a notepad or on a piece of paper should be held securely, as their loss would be a data breach.

If your notepad contains sensitive personal information it must be kept in locked storage when you're not using it. You must shred or burn any pages containing personal information before recycling or throwing away.

10. What do I do with personal information I have in my possession after I stop volunteering?

This should be passed to the person who takes over from you within seven days, or if no-one is taking over your role immediately, then to your Group Coordinator or another named volunteer who has completed the same level of training as the Group Coordinator (see Group Coordinator Welcome and Induction checklist).

Personal data breaches

11. What is a data breach and what do I do if it happens?

A data breach is any situation where personal data is made insecure. In some situations it will be obvious that personal information has been accessed in error, but this is not always the case.

A breach might be caused by:

- Clicking on unsafe links in emails that breach the security of your computer. This may then give access to your contact lists and may also allow corruption to, or damage of data stored.
- Sending an email to a list of contacts using the 'To' field instead of the 'Bcc' field (thereby sharing everyone's email addresses with everyone else, which they may not have consented to, or be happy with).
- Leaving personal information in a public place – either in printed form or on a public or shared PC or smartphone.
- Verbally sharing personal information with someone who should not have access to it.
- A mistake in how an IT system is set up.
- Someone else breaking into or 'hacking' an IT system.

The above list may not include every possibility of a breach, so if you are unsure, you must contact your LNO immediately to report your concern.

If you can't get hold of your LNO straight away, please contact the Data Governance Team on 0203 872 8735 without delay.

12. What if I have done something that resulted in a data breach? Will I be held accountable?

Mistakes happen. If you have reported the breach in good time, and unless the breach was deliberate or negligent, you won't be held personally accountable. Reading guidance such as this FAQ, and if relevant to your volunteering role, completing our Data Protection Essentials online learning, will help all of us to avoid making mistakes.

The important thing is to report the breach promptly so that action can be taken to correct it. We are legally obliged to report most breaches to the Information Commissioner's Office (ICO) within 72 hours.

The consequences, including fines and negative news stories, are much worse if we don't act quickly on a breach.

People who aren't members

13. How do I store and use data for people who aren't members, some of which is sensitive?

We will be asking all groups to store non-members' data on the Portal to ensure that this is kept as securely as the data of people who are members. See using the Portal on our volunteer website for more on this. As with all personal data, you must ensure that non-members' personal information is:

- Stored securely, for example in a locked cabinet or in a private electronic folder.
- Only used for the purpose you originally told the individuals who the information is about, for example, telling someone about forthcoming events.
- That the device it is held on is secure and that files are password protected.

14. I have contact lists in hard copy and electronically kept at home, some going back many years. What do I do with them?

Old contact lists containing personal information that are no longer current or in use must be deleted or, if in paper form, shredded or burned before recycling.

Details held on paper should be locked away in a place with no public access, and lists held in an electronic file should be stored on your computer's hard drive and must be password protected. You can find more information at IT support on our volunteer website

15. Do people who aren't members wanting to receive our newsletter now need to consent to us storing their details?

Yes, and we are legally required to tell all people whose information we hold how we will use their information. We do this with what is called a Privacy Notice which informs the person about our use of personal information.

Look out for the Group Handbook update in May on how to handle non-members requests. This will be publicised in Teamspirit and be available on our volunteer website. Until then please hold any new requests and don't ask for consent.

16. Are there any plans for transferring the non-members' data we hold to the Portal?

Yes and more information will be available on our volunteer website soon. Until then please contact our Data Governance Team if you have any queries.

Members: Data storage and data sharing

17. I have contact lists in hard copy and electronically kept at home. How do I handle (process) them?

Whenever you send information out to your contacts you must download the latest membership contact list from the Portal.

This will keep information secure as well as making sure we don't contact people who no longer wish to receive information from us, or send correspondence to the addresses of people who have died, causing potential distress to family.

The Portal list should be held securely on your computer's hard drive only until you complete the mailing. Securely means that:

- Details held on paper should be locked away in a place with no public access.
- Lists held in an electronic file should be stored on your computer's hard drive.
- The file should be password protected if your computer is not encrypted. If you're not sure how to password protect files or encrypt your computer, see IT support on our volunteer website.

With the exception of MS Society email accounts and Office 365, you must not use cloud based storage (for example, Dropbox, Google Docs or Google Drive) to store personal information and data.

18. I have members' telephone numbers stored on my personal mobile phone. Is this okay?

This is not advisable. However, if the nature of your role needs you to do this, for example, if you are a Volunteer Driver, then you must make sure your mobile phone is pin protected.

If you have personal friendships or socialise with members or other volunteers outside of organised MS events, this is, of course, okay.

19. I give out my home telephone number for use in connection with my volunteer role. Is this okay?

We recommend that groups (and MS Support teams) have a dedicated landline or mobile number to enable you to share responsibility for calls and keep individual volunteer's personal information secure.

IT (email use and storage)

20. I don't use our MS Society email account but one from another provider (such as Hotmail or Gmail). Is this okay?

All email communications with individuals on our behalf should be via your MS Society email account. If this is not practicable (i.e., not yet provided) we advise that you speak with your LNO in the interim; look out for new information about mobile access and group accounts in the next Teamspirit.

21. Why should we use our MS Society email account? What should happen to the information held in previously used accounts (such as Hotmail)?

MS Society email accounts are managed securely and so meet the ICO's requirements. We can't verify the security of information in other accounts.

Recipients may also be confused about whether an email sent via another account (such as Hotmail) is genuinely from an MS Society volunteer and if they are wary of identity theft, may not want to open it.

All emails in old accounts should be deleted so we are sure personal information about our people is not held anywhere but in our own managed systems.

22. What is the difference between our group's general MS Society email account and our MS Support email account? When should I use each?

MS Society email is being updated so that it is easier to use. Find out more in the next Teamspirit.

Only trained Lead/Support Volunteers must have access to your MS Support email account to ensure support enquiries are kept confidential. You should use your general group email for other group correspondence.

23. I have always emailed, and sometimes texted people from my personal email and phone to let them know about social events. Do I need to stop?

You should use your MS Society email account or mobile phone and only text or WhatsApp members who have consented by telling us their preferences when they joined.

These rules apply to official communications on MS Society matters. If you develop friendships with other volunteers or people who access our support and services, you will of course communicate personally using a means of your mutual preference, via your personal device to keep your private and MS Society correspondence separate.

24. Is there an IT course for less IT-familiar volunteers that can be face-to-face and include simple things like how to password protect a file, how to encrypt my computer, how to check a website is safe, etc.?

You can find helpful IT security guidance at IT support on our volunteer website. Many local colleges also offer introductory computer user courses to help people build confidence with using IT and digital tools. Alternatively, ask a friend, family member, or fellow volunteer who is more confident to show you the basics and help you search through the resources available online to help you learn more.

Group Handbook A6: Handling data

25. I don't understand some of these phrases/words. Is there a glossary to explain the meaning and can this be a bit more volunteer-friendly?

You will find a glossary of GDPR terms at the end of this document.

If you are unsure of the meaning of any phrase not listed here, please contact the Data Governance Team in the first instance.

26. The Group Handbook is very long and I don't have time to read it all. How do I keep up to date with the guidance?

The Group Handbook is available to download as individual sections and you'll find everything you need to know about the GDPR in Group Handbook A6: Handling Data. We've also included data protection guidance in other sections, as it relates to specific activities.

The Welcome and Induction checklist for your role will signpost to the relevant training and handbook sections. We recommend you only need to read the sections relevant to your role. The resources are always available so you can go back to them whenever you need to.

See A-Z: Our volunteer roles on the volunteer website for your Welcome and Induction checklist.

Data Protection Essentials online learning complements the Group Handbook and other guidance but is only compulsory for some roles (these are listed in Group Handbook A6: Handling Data).

Your LNO and the Data Governance Team are here to support you if you and/or your group have any questions.

Guidance, policies and Data Protection Essentials online learning

27. What guidance will be available on how we need to comply with the GDPR? When and how will we receive this?

Some volunteer roles have more responsibilities in handling data than others. As mentioned above, your Welcome and Induction checklist signposts to the guidance and training already available.
There will also be new and updated guidance and training available before the 25 May deadline.

Updated Data Protection Essentials online learning will be available in spring 2018 for key volunteer roles and will be publicised in Teamspirit. Your LNO will also be able to give you details.

Other new supporting guidance will be added to our volunteer website as it becomes available and publicised in Teamspirit. The volunteer website will always have the most up to date versions of any guidance, so if you've printed any resources previously, go back to the website to check it's up to date. All resources have a version control box at the end, telling you when it was last updated.

28. I am a volunteer who handles personal data and have completed Data Protection Essentials online learning. Will I need to redo the training for the GDPR?

Yes. Because there are additional requirements for the GDPR which everyone needs to know about, we are updating Data Protection Essentials online learning for both staff and volunteers (see question 17 too). All staff and many volunteers will need to re-do it.

The MS Society is legally required to provide adequate training to everyone who has access to personal data in relation to their role and must be able to show the Information Commissioner's Office (ICO) our training completion records to prove we are compliant with the legislation. Another charity has recently had to pay a large fine for not being able to demonstrate this.

29. Will training on new systems and software be provided, such as Office 365?

As new systems for volunteers are introduced, guidance and support will be provided.

The May edition of Teamspirit will include information on data technology and the GDPR, and will be your next key update.

We are always keen to hear from volunteers about what guidance and support you may need. Contact volunteertraining@mssociety.org.uk to give us your feedback.

Newsletters

30. We try to make our newsletter as attractive as possible, using text and images. Is it OK to re-use relevant text and images from the MS Society website without asking permission each time?

This is fair usage. Groups can use images from our Web to Print library or upload their own images. Ensure you have each individual's permission in writing if uploading your own. You can download a copy of our consent form from the volunteer website.

31. We often list the donations received in our newsletter; some may be organisations, but they are often the name of individuals. Should we seek consent to include the name of the donor?

You should let donors know that this will happen as a matter of course and give them the option not to be listed, or to comment on what you intend to say about them. In some instances, promise of promotion in a newsletter is incentive for donating.

32. How long can we keep newsletters for? And would we ask recipients to dispose of them within a certain period?

Newsletters should only contain information which individuals featured have consented to use where necessary, so they may be kept indefinitely.

33. How long should we keep newsletter data, such as images, stories and consent forms, for?

Consent forms provide a three year period in which you can use the resource for all or either stories, quotes, photos, audios etc., and must not be kept beyond this period. Please store consent forms for a further three years after their expiry in case of enquiries (so that's six years in total). The stories and images you collect are classed as personal information and should be filed and stored appropriately.

34. Can we use sentiments from cards and letters received as testimonials when we need to? Would we now need to seek permission to do so and to name the person?

You should let the person know that you plan to quote from their correspondence giving them the opportunity to object. Quotes should only be used when timely and you should ask each time you want to use the quote and/or name.

If any special characteristics are included or implied, for example, someone's MS status, then you must always check with the person before reusing.

35. Can birthday notifications be included in newsletters?

Birthdays and other personal celebrations should not be announced in newsletters without the individual's permission. A group may send cards to members if you choose to do so.

Passwords and security

36. I was granted access to the Portal after I completed Data Protection Essentials online learning, but I have since been unable to perform my duties. I asked another key volunteer to help and I shared my login details and password. Should I change my password now I am back? Am I allowed to share my password and if not, why?

As you've said, access to the Portal is only granted after completion of Data Protection Essentials online learning. Passwords should not be shared so we know that volunteers who have accessed the Portal have completed Data Protection Essentials online training. If your password has been shared you should change it.

37. Why can't I access information that I was previously able to, such as health information?

As part of our data protection legal obligations, information has to be accessible only to those who need it. Health and other sensitive information have specific rules in the legislation rules under the GDPR.

We also need to ensure that data is appropriately secure, and as health information is extremely sensitive, it needs to be controlled more tightly than ordinary personal information such as an email address.

38. I have one password for all my files and documents. Should I have a different password for each?

It is fine to have a single, strong password for all files and documents held on your own computer, as long as only you have access to this password. Strong passwords are usually a phrase which includes symbols and letters.

Avoid birthdays or other special dates, names of family members or your address.

39. I do not have a locked cabinet in my home for MS Society files and information but my home is secure. Is this adequate? Would the MS Society consider subsidising the cost of cabinets if this is a requirement?

No – you must ensure only people who have had training and need to access information can do so. If you live with others it is likely your home is therefore not secure according to the law.

If you don't have a lockable cabinet, cupboard or room, then your group should purchase the necessary equipment as part of their obligation to ensure you can carry out your role safely. This is considered an appropriate use of funds.

40. We use a family computer at home and I have password protected files on this. The computer is open and anyone (my family) can use it. Should the computer be password accessed as well?

We would recommend that computers are access-controlled with passwords as well. If other family members have access, files must always be password protected.

Third parties

41. What should we do if want to start using a new system or supplier?

You must speak to your LNO before you purchase or start using a new IT system or IT supplier. The MS Society has agreements in place with suppliers who have been verified as meeting the necessary security standards. Only approved systems must be used.

If you want to use a supplier who will need access to any personal information about members in order to provide their service, you must agree how they will hold the information confidentially. The Data Governance Team may need to perform additional enquiries depending on the nature of the service and personal information being provided.

Please refer to our guidance on developing services and activities on the volunteer website.

42. How can we check that our current contractors are handling personal data appropriately? Do we have to stop using them?

You don’t need to stop using contractors immediately. For more information, see the guidance coming soon on developing services here.

Glossary of GDPR terms

Cloud, the
These are apps that allow storage and shared files/interactive work outside of your local computer network, hence the term 'cloud computing'.

Data
In this context, data means personal information, and is a piece or pieces of information which can identify a living person. This personal data includes name, email, address, date of birth and interests. Also see sensitive data (below).

Data breach
Any situation where personal data is made insecure (for example, clicking on unsafe links in emails, sending an email to a list of contacts using the 'To' field instead of the 'Bcc' field, leaving personal information in a public place including on a public or shared PC or smartphone, verbally sharing personal information with someone who should not have access to it, a mistake in how an IT system is set up, or someone else breaking into or 'hacking' an IT system) and puts an individual's information at risk.

Data Controller
The organisation which makes decisions about how data is processed, and has responsibility for ensuring the data is safe and secure and obtained with the right permissions. For example, information collected on Eventbrite is controlled by the MS Society.

Data processing
Includes anything we do to, or with, personal information, such as filing, updating, copying, checking or sharing. Data processing also covers simply storing data even if nothing is done with it.

Data Processor
An organisation processing the data on instruction from a Data Controller. In the example above, Eventbrite is the data processor.

Data Protection Statement
This is the description of the processing of data which is provided to the individual as part of the transparency requirement. The statement includes the purpose of the processing activity and will reference key details such as retention period, what the data collected will be used for, who information will be shared with, and is accompanied by consents and opt-outs. It will also link to our full Privacy Notice.

Data subject
The individual whose data is being processed.

Direct marketing
Communications addressed and sent to specific named individuals in relation to fundraising, campaigning, promoting our aims and ideals, promotional materials, a direct marketing element to a non-direct marketing message, or collecting data for future direct marketing use.

The following activities don't count as direct marketing:

- Administrative purposes
- Genuine market research
- Gift Aid administration
- Management of volunteers and staff
- Maintaining a suppression list

EEA
European Economic Area

GDPR, the
The General Data Protection Regulation. This is the new law for data protection. On 25 May 2018 it will come into force, replacing the Data Protection Act (1998).

ICO
Information Commissioner's Office. An independent public body set up to uphold information rights and enforce compliance with legislation. The Department for Digital, Culture Media and Sport is the ICO's sponsoring department within Government.

Legal basis
We must have legal grounds for processing personal data. At the MS Society, this can be contractual requirement, legal obligation, vital interests, consent of the data subject, or legitimate interests of the MS Society or a third party.

Legitimate interests
A legal basis for processing personal information in line with our organisational goals. Processing must be necessary to achieve this goal, and processing must be justifiable and not override the rights of the data subject. A privacy statement must be supplied to data subjects.

Personal data
Data which can identify a living person or sets of data which, when combined, work together to do the same.

Privacy Impact Assessment (PIA)
A process by which a project or system is assessed to gauge the level of risk to personal data.

Privacy Statement
This is the same as a Data Protection Statement (see above).

Purpose
The reason why you are processing the data. The data statement includes your purpose as it explains to the individual why you are collecting information.

Sensitive personal data or 'special characteristics'
Data such as health information, sexuality and religious beliefs which are given even more protection under the GDPR.

Third party
For our purposes, third parties are any contractors including companies, systems and suppliers that we use to carry out services and functions on our behalf. This may be an individual, a company or software collecting information.

Data protection under the General Data Protection Regulation: Frequently asked questions v1	
Content owner:	Data Governance Officer
Editor:	Volunteer Resources Editor
Sign off:	Data Governance Manager
Sign off date:	March 2018
Review date:	June 2018