



General Data Protection Regulations (GDPR): Frequently Asked Questions

A. Introduction

If you hold and process personal information about your members, bat carers, recorders, useful contacts, etc. you are legally obliged to protect that information and only use it for the purpose it was collected. In order to do this you must:

Only collect information that you need for a specific purpose

Keep it secure

Ensure it is relevant and up to date

Only hold as much as you need, and only for as long as you need it

Allow the subject of the information to see it on request and delete it if asked to do so

The important thing is that you are taking steps to make sure data is secure and using it appropriately and you should document the logic behind the decision you make (or are going to make), including:

How the data was collected

Why the data was collected

How you are going to keep it safe

How you are using it/going to be using it

How you are managing it/going to be managing it (including any deletion/destruction of data)

The questions set out on this web page are based on enquiries BCT have received from bat groups. We have answered these questions to the best of our knowledge and understanding to provide information about GDPR and offer some guidance on the things that you should be considering about the data you hold as a bat group. Different organisations are taking different approaches to the way they deal with data protection, the important thing is to document the logic behind the decision process. We are unable to be prescriptive or give specific advice, however we hope the information in this document is useful.

B. ICO Five Top Tips

Information about GDPR aimed at charities and organisations is available from the Information Commissioner's Office (ICO) website and this includes the following top five tips on data protection aimed at charities (and relevant even if your group isn't a registered charity):

i. Tell people what you are doing with their data

People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice) so it is important you are open and honest with people about how their data will be used.

ii. Make sure your staff [bat group committee members/trustees] are adequately trained

New employees [committee members/volunteers] must receive data protection training to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff [committee members/volunteers].

iii. Use strong passwords

There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep your information secure from would-be thieves.

iv. Encrypt all portable devices

Only move data safely and only when necessary. Make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.

v. Only keep people's information that you need for as long as you need it

Make sure your organisation has established retention periods in place and set up a process for deleting personal information once it is no longer required.

The answers to Frequently Asked Questions below build on these tips in relation to bat group activities.

C. Frequently Asked Questions & Answers

1. Help! We haven't done any preparation for GDPR yet, are we too late?

No, definitely not. The Information Commissioner, in the May edition of the ICO newsletter, stated: "To...clubs and associations who are not quite there, I say ... don't panic! As the new ICO Regulatory Action Policy, out for consultation very shortly, sets out, we pride ourselves on being a fair and proportionate regulator. That will continue under the GDPR. 25 May is not the end of anything, it is the beginning, and the important thing is to take concrete steps to implement your new responsibilities – to better protect customer data." Customer can be taken to include bat group members, other contacts, those people who provide records, etc.

This is all a work in progress and the most important thing is to have a plan for how you will make sure your bat group is compliant with GDPR and for that to be put into effect as soon as possible.

2. Do we need to ask all our members if we can continue to contact them?

If people have paid a fee to join your bat group, then holding their information and communicating to them about the activities of the group is a legitimate interest, your members have actively opted in to becoming a member and receiving emails from the group is a reasonable expectation. Therefore you don't need to contact members to ask if they want to remain on your contact lists.

You should record how you handle members' data and how you use it in a data privacy notice process that you do share with your members. The "How can we apply legitimate interests in practice?" section in the ICO site is quite useful (and see question 3. below).

3. I've read somewhere that all organisations need a privacy notice? Does that apply to bat groups and if so what should it include?

Yes, you should have a privacy notice for your bat group that you share with members and with anyone else whose data you hold (e.g. where you hold bat records that include people's details). According to the ICO, the starting point of a privacy notice should be to tell people: who you are; what you are going to do with their information; and who it will be shared with.

Some suggested headings to include in your privacy notice are:

Introduction – what the privacy notice is, an explanation of personal information and who you are (e.g. bat group committee or trustees).

What type of personal information does the bat group hold – members contact details, bat carers details, etc. This should be the minimum that you need to manage someone's membership (see question 8. below).

Why the bat group holds that information – for example to administer memberships, to inform members about events and activities, etc.

How long you keep that information for – as long as someone is a member, for as long as is required for financial reasons, etc.

How you will manage data – for example if you have mailing lists for non-members how often will you get in contact with people to see if they want to remain on that mailing list (see question 5. below); how long after a membership has elapsed will you delete the persons details, etc.

What are the grounds for the bat group processing personal data – there are legitimate interests for holding personal information, this may include things like managing memberships, keeping complete biological records (where the 'who' is a core part of a record), safeguarding, etc.

Who data is shared with – for example bat records could be share with your local records centre.

People's rights in relation to their personal information that you hold – such as accessing the data you hold on them.

How people can get in touch – contact details if they have any questions about the privacy notice, the data that you hold about them, etc.

[Back to list of questions](#)

4. We've drafted a privacy notice but do we just need to share it with members once?

You should certainly make sure your members see the privacy notice you have prepared, for example by emailing it to all of your members. If your group has a website then it would be good to include it there as well. You could include a link to the notice on your website at the end of your emails. Share it with new members when they join. You should also provide it if requested by any of your members or anyone else whose information you hold. If you update it then you need to let the relevant people know it has changed and provide a copy.

If you would be happy for your bat group to share its privacy policy with other bat groups please email Lisa Worledge who can organise this through the bat group pages of the BCT website.

5. We don't have paid memberships as such, just an emailing list, do we need to contact everyone to ask if they want to stay on our contact list?

Yes, you need to contact them to ask if they are happy to continue receiving communications from the group. People need to actively opt in if they aren't paid members of the group and if they don't respond then they need to be removed from the mailing list.

In your email give a brief description of how the data will be used (e.g. to keep people updated with bat group activities, events, fundraising and other relevant information) and what it won't be used for (e.g. the bat group will not share your information with any other organisations).

Give people a reasonable time to respond but then delete them from your records if they haven't responded within the time period or if they have asked to be removed.

As stated in response to question 3 above, you need a policy in place that if someone opts in then how often will you ask them again, it is reasonable to expect to be asked every 2-3 years. This can be mentioned in the original email and of course you should say to people that they can opt out at any time by contacting getting in touch (and give the relevant contact details).

6. I like to keep good records and I have always kept records of lapsed members in case they ever want to join again or we may want to get in touch. It sounds like I can't do this under GDPR, is that correct?

That is correct, you can't just retain data because you like to. The key here is having a legitimate justification for holding that information. Basically for any data you hold you need to have a good reason as to why you are holding it and if you don't you shouldn't hold that data. An example of a legitimate reason is to manage someone's membership but if that person is no longer a member then why do you need to retain their data?

There may be a financial reason for holding data about a membership after it has lapsed, the suggested period for the retention of financial information is seven years, but you shouldn't be contacting people if they are no longer members (or for non-members), if they haven't opted in to receive communications. There is no legitimate interest for that communication. You also need to make sure you have a process in place so that after seven years that data is deleted securely.

It is a good idea to set-up an annual admin review and a tidy up of records to make sure you aren't holding onto data that you shouldn't be. This can be built into your privacy notice (see question 3. above).

7. We send an annual email to former members to see if we can tempt them back, is that okay under GDPR?

If people have lapsed memberships and you want to continue contacting them, you should send them an email to ask if they are happy to continue receiving communications from the group. People need to actively opt in if they aren't members of the group. If they don't respond then they need to be removed from the mailing list. (See the answer to question 5. above).

In the future, if you want to contact former members to see if they would like to rejoin the group, then going forward you should have something on the group's membership form that says the group will contact people for up to x-period after their membership ends.

8. What data can we hold about our members?

You should ask yourself the question what information do you need to hold to manage someone's membership? It could be as little as their name and email address (if you don't send any postal communications). If you need to hold more information than you need to make sure it is justifiable, for example you may hold age or at least a note that people are over 18 (see question 10. below).

9. Can we still hold people's names as part of the bat records we hold and/or pass on to our local records centre?

It is an accepted scientific principle that a biological record includes who recorded it, i.e. the recorder's name, as a minimum a biological record is of what, where, when and who. If you agree and that is your argument for holding that data then you should document that decision and make a statement as to why you need to hold it.

Going forward you should include a statement in communications with people submitting records to check they are happy for their name to be shared, for example if you are passing on records to your local biological records centre.

You need to consider who is accessing your biological records data, what information you are sharing when doing data searches for other organisations (for example do you need to include the name of the recorder if you have verified the record). If you do need to include it and the person who provided the record has consented to their data being shared in that way then that is fine but you should keep records of that consent. If they haven't consented then you should not be passing on their name with the records to third parties until you have consent.

You should be able to get more information about GDPR relating to biological records from your local biological records centre. The key, as with other aspects of GDPR, is to document your decisions and what you are doing (see question 3. above).

[Back to list of questions](#)

10. We have members of all ages, is it okay to hold data for our members who are under 18?

You cannot store the details of anyone who is below the age of 16 unless their parent or guardian has specifically consented to it. So if you have a family membership and parent or guardian has given children's names when joining, that is fine but if you have an individual membership for someone below the age of 16 then need to get consent from their parent or guardian to hold that data and to contact that person.

11. I have been meaning to have a sort out of emails for a long time – are there any GDPR implications in the fact we have emails from members of the public and other people going back a few years?

For old emails (and indeed current ones for that matter) you need to consider whether the data being protected properly? You must ensure that the data can't be used maliciously by anyone within the bat group or externally e.g. is your email password protected, is it a strong enough password, do you change it regularly, if it is a shared email account, how is access controlled?

If the emails aren't being used for anything then why are you keeping them? Going forward you need a plan about dealing with old emails and you should document what you will be doing (see question 3. above). You could include a statement in your email signature for replies that states enquiries will be held for x-period of time. You should explain why and the framework under which you are keeping it, e.g. how you are going to use it and why are you are storing it.

12. We often get people signing up for further information about bats at events we attend. Are we okay to retain their information?

On your sign-up sheet for further information you should have a statement at top about how you are going to use data or even have a piece of paper they can take away. For example you could make it clear that you won't be sharing their contact details with any other organisations, that's you'll be retaining the information for x-period of time (unless they consent to continue receiving communications), and you should include a statement on how you are going to use that data e.g. to send an information pack, be added to an emailing list (from which they can opt at any time).

For any non-membership contacts you already have (e.g. media contact with local radio station or newspaper, landowners, event organisers, etc.) then you need to send them an email out to ask if they are happy to continue receiving information from the group/be held as a contact (see question 5. above). Even if you are not going to be proactively sending people information routinely you still need some sort of consent to say people happy to be contacted in future (for example with stories of interest if a media contact).

13. We have lists of people who have taken part in surveys, who are happy to volunteer on stands, who do bat care, etc. can we keep all these separate lists?

You need to think about how the data has been collected and how is it being used. You should document why you are keeping it (e.g. so that you can invite those people to the next event) or why you are deleting/destroying any data.