Data safety & GDPR for Meetings

EU GDPR – intro to the legislation

In May 2018, the EU General Data Protection Regulation will come into force. It will also be enacted by a new UK Data Protection Act (so even though the UK will be leaving the EU, the regulation will still apply).

The ICO has published very useful guidance on the GDPR and related issues. Please read for more information: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ (They have also set up a helpline for small organisations).

The Fundraising Regulator has also compiled some very useful guidance here: https://www.fundraisingregulator.org.uk/information-registration-for-fundraisers/guidance/data-protection-library-general-data-protection-regulation-gdpr/

Proportionate response

Meetings should bear in mind, that the ICO advice on data protection has always emphasised a reasonable approach (what can be reasonably expected by data subjects) and proportional actions (what is realistically achievable by organisations). Small organisations run by volunteers cannot reasonably be expected to follow the same data protection regime that a large organisation with IT support, information

*Meetings may take the view that long standing, active attenders can be administrated under legitimate interests as with members, and that they do not need consent to hold personal data that an attender might reasonably expect to administrate the meeting. This is for meetings to decide but should be defensible under the regulation.

management professionals, large budgets etc can. So, while we should take some practical steps to improve management of personal data, there is no need to panic.

There are several changes to data protection legislation that meetings should be aware of:

Accountability and governance

The GDPR states that we must be able to demonstrate our compliance with the regulation and be accountable to data subjects and regulators.

This means we should have written policies and procedures in place in regards to personal data and that we should communicate these to members, attenders and any other persons we collect data from.

Consent

The GDPR has brought in stricter rules for obtaining consent. From May 2018, when you are asking consent for data collection, it must be explicitly given (opt-in, not opt-out) and you must provide more contextual information than before. *See consent checklist*.

******However, for many activities carried out by meetings, you may not require consent. See below. ******

FAQs

Do we need to have members' consent to hold their personal data?

Consent is only one of several legal bases for processing personal data. The ICO advises that organisations **should not** rely on consent if their activities fall under another of the legal bases.

The most relevant legal basis for local and area meetings is:

Legitimate interests (necessary for the core administrative functions of the organisation, reasonably expected by the data subject, not prejudicial to a person's rights or likely to cause harm)

*Meetings may take the view that long standing, active attenders can be administrated under legitimate interests as with members, and that they do not need consent to hold personal data that an attender might reasonably expect to administrate the meeting. This is for meetings to decide but should be defensible under the regulation.

Data safety & GDPR for Meetings

This basis for processing coupled with the exemption for special category processing which allows an organisation to process sensitive personal data if it is:

"*processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects*"

should mean that **most activities of the meeting do not require consent**.

We are advising that for members of the Society, there is a reasonable expectation that the meeting will hold some personal data for the purposes of necessary administration of the meeting.

For attenders*, you should ask for consent to hold their data. (see 'how to ask for consent' below).

For children, you should ask the permission of the parent or guardian to hold their data. (see 'how to ask for consent' below).

Remember that Quaker Faith & Practice (Qf&p 11.37), and charity best practice, requires that a **permanent record of membership** is maintained by each meeting. A register of members (not published or shared) should be created regularly and archived for permanent preservation. This is not the same as the members' contact lists/book of meetings created for sharing more widely which does require consent.

Other legal bases may apply to some meetings, such as 'performance of a contract' including contracts with employees – again you would not need to ask for consent to processing the data involved in this instance (such as applications forms, CVs etc).

You can read more about this here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

What should we ask for consent for?

*Meetings may take the view that long standing, active attenders can be administrated under legitimate interests as with members, and that they do not need consent to hold personal data that an attender might reasonably expect to administrate the meeting. This is for meetings to decide but should be defensible under the regulation.

Data safety & GDPR for Meetings

The meeting should decide what activities they deem as core functions and therefore necessary administration of their meeting, and for these activities you **do not** need consent. This may include:

- membership and nominations administration
- contacting members regarding holding of meeting for worship (e.g. change of time)
- pastoral care through eldership and oversight
- fundraising from members
- etc.

To decide which activities fall under legitimate interests, it is useful to carry out a personal data audit as a meeting. ***See data audit guide***.

Again, for attenders, you should ask permission to contact them or use their data for these activities.

For any activities the meeting decides are *above and beyond* the necessary administration of the meeting, you should gain consent to use the data. This may include:

- Promotion of BYM work and events
- Promotion of events or services by other organisations or private individuals (Woodbrooke, other Quaker bodies, non-Quaker organisations, babysitting service run by a member etc)
- Requests for donations from non-members

You should document these activities so everyone is aware what they are. A good way to do this is by creating a privacy notice for your meeting. See ICO guidance on creating privacy notices: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/

How do we ask for consent?

When you ask for consent to collect and manage someone's personal data, you should:

- Explain why you are collecting it – list all the ways in which you will use it

*Meetings may take the view that long standing, active attenders can be administrated under legitimate interests as with members, and that they do not need consent to hold personal data that an attender might reasonably expect to administrate the meeting. This is for meetings to decide but should be defensible under the regulation.

Data safety & GDPR for Meetings

- Explain how you will manage it and how long you will keep it for (if you use personal computing to store the data, explain this, if you only keep it in paper form, inform them where it is kept).
- Explain how they can withdraw permission and ask for the data to be deleted (who do they contact to do this?)
- Explain who they should contact should they wish to make a complaint

You need to:

Make sure you have the procedures in place to manage personal data correctly – secure internet systems where possible, procedures for who can access what information, deletion of data that is no longer used, complaints procedure etc.

Also it is very important that *if* you ask someone's consent to keep their data – you keep the record of the consent for as long as you keep the data.

See template consent forms at http://www.quaker.org.uk/our-organisation/support-for-meetings/data-safety

Do we have to backdate consent?

Where you have decided you need consent to hold personal data (such as attenders' consent or for a mailing list about services offered by external organisations), if the original consent does not meet the standard set by GDPR, you are best to ask for this consent again with the new necessary contextual information required by GDPR.

There is some risk management involved here. If you are confident the people on your mailing list understood what they were signing up to, and have a clear way to unsubscribe, you may weigh up whether you are happy to continue on that basis rather than annoy users with unnecessary red tape.

Can we share personal data?

With third parties?

It depends somewhat on the third party. Would your member reasonably expect you to share the particular data with the third party?

*Meetings may take the view that long standing, active attenders can be administrated under legitimate interests as with members, and that they do not need consent to hold personal data that an attender might reasonably expect to administrate the meeting. This is for meetings to decide but should be defensible under the regulation.

Data safety & GDPR for Meetings

Have you taken reasonable steps to check your suppliers comply with GDPR? (Enquiring about procedures, checking their privacy policies, in some cases asking for written agreements)

Examples:

In the case of booking a venue for an event, you may decide that everyone who booked onto the event can reasonably assume that you will share their basic info and dietary needs with the appropriate venue staff.

Would your members expect you to share a list of their contact details with a member who wants to advertise their florist business? – Probably not.

Cloud services such as dropbox, google groups etc?

Under GDPR all companies who manage EU customer's data are required to be compliant with the regulation, however it is currently somewhat of a grey area. We hope that these US based companies will be GDPR compliant before May 2018.

Use of these companies may be a risk the meeting has to weigh up – can you operate successfully without using them? Are there EU-based alternatives? What are the risks involved? What types of data might you be willing to store on these services and what would you not be willing to share?

Do you ask consent for use of these from all involved?

Contractors such as accountants, auditors etc?

We take the view that for the period you contract these types of services they are basically 'employees' of the meeting and therefore it is not 'data sharing' as understood under data protection legislation. Obviously safeguards should still be in place to ensure we use reputable contractors and that they don't continue to hold data after their business function has been completed.

GDPR – checklist of actions meetings can take to prepare

*Meetings may take the view that long standing, active attenders can be administrated under legitimate interests as with members, and that they do not need consent to hold personal data that an attender might reasonably expect to administrate the meeting. This is for meetings to decide but should be defensible under the regulation.

Data safety & GDPR for Meetings

- Carry out a personal data audit
- Create a privacy notice to share with all stakeholders
- Create written policies and procedures (where appropriate) for managing personal data such as:
    - Employee and volunteer data policy
    - Complaint and data breach procedure
    - Safeguarding data policy
    - Event data policy

Historical archiving

The Society of Friends has a strong tradition of recordkeeping and a wealth of historical records, both those held centrally in Library of Society of Friends in London, and meeting records held in record offices in England, Scotland and Wales.

Meeting records which are traditionally selected for historical archiving and research include:

- Minutes (of all committees including elders and overseers)
- Membership records (often including applications and visit records)
- Registers of members, births, marriages and burials
- Financial records (charity best practice advises records such as annual accounts are preserved for the lifetime of the organisation)
- Etc

This tradition is not threatened by data protection legislation as there is an exemption for historical archiving and historical research. Records may contain personal data, even sensitive personal data, but they should still be preserved for historical record.

*Meetings may take the view that long standing, active attenders can be administrated under legitimate interests as with members, and that they do not need consent to hold personal data that an attender might reasonably expect to administrate the meeting. This is for meetings to decide but should be defensible under the regulation.

Data safety & GDPR for Meetings

*Meetings may take the view that long standing, active attenders can be administrated under legitimate interests as with members, and that they do not need consent to hold personal data that an attender might reasonably expect to administrate the meeting. This is for meetings to decide but should be defensible under the regulation.