BYM Data Protection handbook for Meetings

Created by BYM Data Protection Group. Updated 2019.

The BYM Data Protection group have compiled this handbook to give some advice to meetings about data protection issues. We work on Data Protection compliance for Britain Yearly Meeting, and have spoken to many meetings about their ways of working, and data protection issues they face. We hope we will cover the main areas of concern for meetings.

All roleholders should have an understanding of how Data Protection affects Area and Local meetings. While some roleholders will need to consider data protection more than others do, anyone processing personal data on behalf of the meeting should familiarise themselves with the basic principles.

Contents

BYM Data Protection handbook for Meetings

Created by BYM Data Protection Group. Updated 2019.

Introduction to Data Protection legislation

In May 2018, the EU General Data Protection Regulation (GDPR) came into force. Later that year the UK Data Protection Act 2018 replaced the previous Data Protection Act 1998, and enshrined the principles of GDPR into UK law. For that reason, for the rest of this handbook we will refer to the UK Data Protection Act 2018 (DPA 2018) as it has established the same principles as the GDPR for the UK data environment.

The seven basic principles are:

I. **Lawfulness, fairness and transparency**: you are open about the data you collect and you treat it, as you would wish your own data to be treated.
II. **Purpose limitation**: you only collect data for the purposes you state, and only use it for that purpose.
III. **Data minimisation**: you only collect the data you need to do the task (do not collect more data than you need).
IV. **Accuracy**: you keep accurate and up-to-date data.
V. **Storage limitation**: you only keep data for as long as you need it for the original purpose (although there is an exemption for historical archiving).
VI. **Integrity and confidentiality**: you do everything in your power to ensure data is kept secure and confidential.
VII. **Accountability**: you document your policies and procedures so you can show how you have treated personal data you process.

For more information: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

The changes brought in in 2018 are not vastly different to the previous regime under the DPA 1998. The main changes are a tightening up of procedures for giving consent, and an increased focus on documenting how you comply (having actual written policies and procedures).

The Information Commissioners Office (ICO - https://ico.org.uk/) is still the regulator for the UK. Their approach remains the same and is a reasonable one. They understand that organisations can only respond according to their resources, and their enforcement of compliance is proportionate to the size of the organisation and the spirit in which they operate.

Our main message for meetings therefore, is that Data Protection is something that aligns with the values of Quaker meetings – we want to treat people fairly, and that includes processing personal data with care. We should understand data protection and have simple policies and procedures in place to ensure we treat personal data correctly. However, meetings are small volunteer-run organisations with limited resources; we cannot expect to meet the standards of large organisations with staff and IT systems etc. There is no need for panic or to restrict what you do unnecessarily.

Registration and governance

Organisations who process personal data have to register with the ICO. There are exemptions for some organisations (mainly based on size and types of activities they perform). The ICO has a simple self-assessment tool to check if you have to register or not. The tool is here: https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/

Our understanding of the above assessment tool is that if Area and constituent Local meetings **only** process the data of members and attenders, you may be exempt from registration. If however you collect data from the public, room/event bookings data, employee data or anyone else's data other than members/attenders you will probably qualify for registration.

Previously we thought that Area Meetings who were not charities could ‘come under’ the BYM registration but this is not the case. Therefore, all Area Meetings should take the above self-assessment to see whether they should register. There is an annual registration fee of £40 for small charities.

Area Meetings own the business records of the Local meetings under them, and therefore are ultimately responsible for the data processing at area and local level. The Area Meeting is therefore the Data Controller and responsible for data protection compliance at area and local level.

Relationship with Britain Yearly Meeting

Britain Yearly Meeting has decided that some of the processing of personal data of people in Meetings is in the legitimate interests of our work and therefore does not require consent for its collection. This includes:

- Basic information for members (Name and Meeting they belong to)
- Personal data required for the nominations process (Name, contact details, some biographical information)

Without collecting this data, it would be very difficult to perform some of the basic functions of the Religious Society of Friends, and achieve the particular objectives of Britain Yearly Meeting in relation to supporting meetings and the Church nationally.

Further personal data such as contact information and attenders’ data is collected by Meetings and passed to Britain Yearly Meeting with the consent of those data subjects. See section below on consent.

Frequently Asked Questions

Consent

Do meetings need consent to collect personal data?

In most cases, no.

Under GDPR, consent is only one of several bases for processing personal data. The ICO advises that organisations should not use consent as a basis for collecting data if

one of the other bases applies. The other bases, which are most likely applicable for local and area meetings, are:

- **Legitimate interests:** this means data processing that is necessary for the core administrative functions of the organisation, reasonably expected by the data subject, and not prejudicial to a person's rights or likely to cause harm.
  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* [that] *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*"[1]

  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.

- **Performance of a contract:** this means data processing in order for two parties to fulfill their obligations to one another. Under GDPR, the contract does not have to be a written one. This could include employment, volunteering, room bookings etc, as long as the data is relevant and limited to what is necessary for the exchange of services and processed in accordance with the seven data principles.

[1] This description of a membership organisation allows meetings some leeway with how you categorise attenders. Regular, long-term attenders can be treated as *de facto* members; this may mean you do not require their consent for data collection for the necessary administration of the meeting. Where you draw the line between a short-term and long-term attender may be difficult though, there is no guidance on this, so it is at the discretion of the meeting.

What should we ask for consent for?

You should ask for consent for processing activities that go *beyond* the administration of the meeting. This could include:

- **Distributing contact lists** - most meetings ask consent to add people's contact information to a widely distributed contact list (this should not be confused with contact lists used only by roleholders for necessary administration, nor the permanent record of members, neither of which require consent).
- **Data sharing** – if you want to share personal data with third parties you should also ask consent (for example sending list of contacts to Woodbrooke).
- **Marketing** – if a local business or charity wants to send information to members of the meeting, you should ask their permission before giving over their contact details.

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

- 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 subjects how it is kept).
- Explain how people 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 about how their data is handled.

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 Data Consent form for meetings.

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 over-burden people with unnecessary administration.

Members' and attenders' records

It is advised in Quaker faith & practice that meetings should keep a permanent record of membership (traditionally referred to as the Register of Members); this is also advisable to comply with charity best practice.[2] This does not require consent.

This activity should not be confused with:

- Compiling internal contact lists for administration, which can be continually updated (and would also not require consent);
- nor with the contact lists (traditionally referred to as the Book of Members) created for distribution widely among the meeting (for which we usually advise seeking consent).

[2] *Quaker faith & practice, 11.47* https://qfp.quaker.org.uk/passage/11-37/

Under the description of membership organisations in GDPR, there is a useful description:

"*the members or the former members of the body or to persons who have regular contact with it in connection with its purposes"*

which we think allows some room for meetings to consider long term attenders as 'members' in relation to some data processing (and therefore potentially not require consent, such as keeping their contact details for necessary administration of the meeting under the legitimate interests basis for processing).

Children's records

We advise, after consultation with meetings, and the BYM Children and Young People's team, that meetings consider children as aged under 16. Young adults aged 16 and over can give consent themselves for processing of their own data.

Data sharing

Whether or not it is ok to share personal data with others depends somewhat on the third party you wish to share it with. You need to assess the purpose for which you hold the data, the nature of the data sharing, and what would be reasonably expected by the data subject. Refer to the examples below.

Example 1: You have booked an external venue for a summer party and members/attenders have filled in booking forms to attend. The venue ask for names of attendees and any special requirements for accessibility and dietary needs. It may be reasonable for the people booked onto the event to assume you will share this data with the venue as part of the event administration.

Example 2: A local funeral director contacts you and asks for postal addresses of meeting members so they can send flyers advertising their service. Would your members expect you to share a list of their contact details in this case – probably not.

You should also take reasonable steps to check those you share data with comply with GDPR (enquiring about procedures, checking their privacy policies, in some cases asking for written agreements).

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.

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 share/store on

these services and what would you not be willing to share/store? Have you given guidance to people on how to use the service?

Do you ask inform data subjects that you use these services? This could form part of a privacy policy for the meeting.

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 do not continue to hold data after their business function has been completed.

Sensitive data in minutes and reports

There is no reason not to include sensitive and personal data in minutes and other administrative documents if it is necessary to give a full record of the business of the meeting, or of decisions taken. This data should be accurate and factual rather than hearsay or personal opinion.

You then should take necessary steps to ensure these records are kept securely and confidentially, and only accessed by relevant roleholders.

We advise meetings to deposit their records on a regular basis with their local record offices (and to Friends House in the case of London & Middlesex meetings). They should be deposited under a 50 year closure, and in the case of particularly sensitive records, such as elders/overseers, childrens, membership reports etc, under a 100 year closure.

Rights, breaches, and complaints

Rights

Under GDPR data subjects have the right to ask you to do various things with their data. The various rights are explained in detail by the ICO here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

They are as follows:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability

- The right to object
- Rights in relation to automated decision making and profiling.

The most common ones meetings will face, is the right to rectification, where people will ask you to update their details – this is simple to deal with and should not cause any issues.

People may ask you to stop processing their data. This usually means people want to stop receiving mail or contact from the meeting (not that they wish all their data be deleted).

People may also ask for copies or access to all the data you hold for them (right to access - usually referred to as a *subject access request*). This can be more difficult to comply with. *See guide to subject access requests.*

People may also ask you to delete all their data (right to erasure). In many cases you will not need to comply with this request fully, for example it would not be possible or reasonable to delete all minutes that feature someone's name. This is not the type of action that this right was created to support.

In all cases, if you receive a request under one of the above rights and are not sure how to proceed, please contact BYM Data Protection Group for advice.

Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

It can range from accidentally sharing email addresses publicly with a group of people (rather than hiding them from view using BCC), to leaving a paper contact list on the bus, to more serious theft of personal details, or computer hacking.

It may be an accident by someone in the meeting, or it may be beyond the control of the meeting (e.g. a burglary).

You may discover the breach yourself, or someone affected or someone who has noticed it may report it.

The important steps to take are as follows:

- Identify cause of breach and take measures to contain it/fix the issue
- Assess potential risk associated with the breach
- Contact data subjects involved to inform them of the breach and what measures have been taken to solve the problem or rectify the situation
- Decide whether the police or the ICO should be notified

The response will vary according to the type of breach.

Example 1:

Someone in the meeting accidentally emails a staff member at Woodbrooke with several email addresses of people copied in, who did not consent to their contact details being shared with the Woodbrooke staff member.

One of the people involved is upset by this and complains to the meeting. The original sender of the email had not noticed that they had shared the emails publicly rather than using the BCC function.

Response: Mistake has been identified. Risk is assessed as low; although someone has been upset by this sharing of their contact details, the risk of harm to them is minimal. All people involved have been emailed to alert them to the mistake, and apologised to. The staff member at Woodbrooke has been asked to delete the email to contain the breach. All roleholders are asked to read over some tips on email security.

Example 2:

Someone has broken into the Meeting House and two laptops and an external hard drive have been stolen. The external hard drive was not password protected or encrypted. The laptops were password protected.

Response: Break-in identified. Risk assessed as medium. Police are called, and ICO is informed. All meeting members/attenders whose data was thought to be on the laptops and hard drive are informed. Meeting decides stronger guidance on password protection needed; encryption of mobile devices with meeting records is new policy; improved security at Meeting House, hard drive now in lockable cupboard.

Complaints

Under GDPR people have the right to complain about how their data is handled. You should clearly state who people should contact if they wish to complain and think about your process for handling complaints.

When you respond to a complaint you should advise people that if they are still unhappy with the situation, they have the right to contact the ICO.

With all requests, breaches, and complaints, GDPR requires us to document these and the responses to them. Meetings should minute how they have handled requests, breaches and complaints.

Archiving and historic records

There is an exemption under GDPR for historical archiving that over-rides the principal of only keeping data until it serves its purpose.

However, it is best to comply with this principal by keeping a list of the records the meeting considers worthy of historical archiving. This can be a simple list, or can be done as part of a data audit or retention schedule. There is more advice on recordkeeping on the record custodians' page on the website: https://www.quaker.org.uk/our-organisation/quaker-roles/records-custodians-librarians

How to ensure your meeting is compliant

Data audit

Under GDPR organisations should keep a record of their processing activities. We have referred to this as a data audit; a document where you list the functions the meeting does which entail collection of personal data; the purpose for the function; the legal basis for the function (legitimate interests, performance of contract, consent); where the data is stored and how it is managed.

The document should be referred to and updated regularly in case processes change or more functions are created. This document will provide the basis for your data protection and privacy policies.

See templates for an example data audit.

Data Protection policy

Under GDPR organisations should have a general data protection policy that is an internal document so everyone in the organisation understands their responsibilities for compliance. It should set out how you aim to comply with the seven data protection principles.

See templates for an example data protection policy.

Privacy policy

Under GDPR you should publish a public privacy policy explaining to data subjects how you will manage the data you collect from them. If you have a website there should be a copy there; if not you should attach a copy to wherever you collect data.

A privacy policy sets out what data you collect, for what purpose, and how you intend to manage it to comply with the principles of data protection. It also advises people how to make requests, such as updating their data, and how to make a complaint.

See templates for an example privacy policy.

Retention of records

You should ensure you have systems in place whereby personal data that is no longer required is destroyed in a secure manner, and personal data that is required

for long-term retention is identified and kept securely, including transfer to archives if required for permanent retention.

If you have a records custodian they may have already created a retention guide or schedule, as per the guidance for custodians: https://www.quaker.org.uk/our-organisation/quaker-roles/records-custodians-librarians.

Although record custodians arrange for the transfer of permanent records to archives, all roleholders and administrators need to ensure timely destruction of personal data which is not required for retention.

Where to find more help

The ICO is the main source of help for organisations and individuals. They have a range of guides, resources and templates. They have also set up a telephone helpline specifically for small organisations.

Main website: https://ico.org.uk/

Helpline: https://ico.org.uk/global/contact-us/advice-service-for-small-organisations/

There are other websites aimed at small charities that are also good sources of support:

Round-up of advice from the internet aimed at small charities tackling Data Protection. It includes links to free templates. https://www.smallcharities.org.uk/783/

National Council for Voluntary Organisations – lots of guidance and help including training offered:
https://knowhow.ncvo.org.uk/organisation/operations/dataprotection#

Charity Finance Group guide to compliance https://cfg.org.uk/GDPRGuide

You can also find many organisations data protection policies online, and most webpages will have a privacy policy link on the footer of the page, so you can see how other organisations are approaching data protection.