Subject Access Request procedure – Meetings

Created May 2019
Updated January 2020

Support available:

Please contact **BYM Data Protection Group** at dataprotection@quaker.org.uk for advice and support dealing with any requests.

ICO advice: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

The ICO is working on a new code of practice for subject access requests but this is still under consultation (as of January 2020) so keep an eye on the release of this guidance.

First response to a request: Confirmation of receipt and clarification

You should start by sending a formal response to say you have received the request and will respond within one month (this should be in writing but can be an email). You need to keep a 'paper trail' of the entire process (again can be in digital format).

You do not need to give any further information other than to confirm you have received the response. You have one calendar month from the date of receipt of the request to respond. It is better to send a holding email to confirm so you have time to think carefully about the response than try to give a panicked answer.

It is good practice to use only one lead contact person for all communication so there is no confusion.

Clarification – it is a good idea to make sure you clarify what exactly the person is requesting as there are several rights under GDPR and people tend to confuse them. People do not have to make their requests in formal language or using the language of Data Protection legislation, so requests can be vague.

The rights are:

1. **Right to be informed** (This just means the person has asked how you are managing their data, and what you are using it for. They are not asking for copies of the data or for any changes or deletion).
2. **Right of access** (This is what is known as a data subject access request (DSAR) and is when someone requests copies of all the data you hold on them – will discuss further below).
3. **Right to rectification** (This is when someone wants you to update their info or change their consent).
4. **Right to erasure** (This is when someone wants you to delete their data that you hold. Meetings will rarely have to do this – there are many exceptions to

complying with such a request. If you receive such a request, contact BYM Data Protection Group for advice)

5. **Right to restrict processing** (This is when someone can ask you to stop processing their information but not to delete it. In many cases someone asking for their information to be deleted should be directed to make this request instead (i.e. it is usually unreasonable to delete every reference to someone from Meeting records, however it is reasonable for someone to request that they are never contacted again by the meeting, and their details are removed from all current contact lists/admin records etc)
6. **Right to data portability** (This is when someone wants a copy of their data in a transferable format so they can use it for something – unlikely a meeting will get this request).
7. **Right to object** (This is the right to complain about how data is being handled. We usually say you should try to deal with the complaint first and allay the person's concerns, but if they are still unhappy you are legally required to inform them of their right to take the complaint to the ICO).

Some of these are much simpler to deal with than others, so clarifying what the person wants, before panicking about having to do a full subject access request, is important! The person may also not actually want to make a formal request at all, but may have asked a question which sounded like one.

Identity

You may also want to ask the person to prove their identity before you release the data to them. Be aware that it is easy to set up an email address in any name, so this is not proof of identity. They can do this by sending you a photo of their driving license/passport, for example.

What you have to provide

If you have established that, the person is making a right to access / subject access request, the aim is to try to collate all information where the requestor's personal data is recorded and give the person copies of this data within one month.

However, the law is reasonable. For example, if the person has been involved with the meeting for 30 years, and you have 25 years of paper-only records that are not name indexed, you are not expected to manually read the minutes to find every mention of the person's name. *Remember data protection legislation is primarily concerned with digital information, and paper records where they are easily searchable.*

You also do not have to provide (and should aim not to without their permission) other people's data as part of a request. So for example, if the person's data appears on a MS Excel spreadsheet as part of a contacts database, you should not send them a copy of the database, or an image of the spreadsheet. You could send an edited screengrab so they can only see their line of the spreadsheet, or type out the

information recorded on the spreadsheet, and tell them it is held within an Excel spreadsheet.

Likewise, if someone is mentioned in emails – you should probably print the emails, redact data for other people, then give a redacted version. (Beware, if you just print, redact using marker, then give the person that page, you can usually read through the marker pen – better to redact with marker, then scan or photocopy; or use redaction software if confident to do so).

You should be careful about releasing documents where, even after redaction, it would be possible to work out who the third parties were. This may pertain to Meetings especially, as they are small communities. You need to weigh up any sensitivities or consequences of releasing documents with others' data.

BYM have withheld documents entirely where it would be possible to guess the third parties' identities, and where there are particular sensitivities, such as communications to us complaining about a subject's behaviour in meeting, where we feel we owe a duty of confidentiality to all involved. This is another complex area, which must be assessed on a case-by-case basis for each document.

The ICO has some guidance on 'complaints' files which may be useful: https://ico.org.uk/media/1179/access_to_information_held_in_complaint_files.pdf

How to find data

This will vary greatly from meeting to meeting. The steps would include:

1. List all the record types where the data might appear (eg. AM main minutes; LM main minutes; register of members; contacts database; elders/overseers minutes etc etc)
2. Then note where this data is located
3. Appoint people or a person to make searches of each record type for the name
4. Record each case where it appears
5. Assess how copies of each record could be made; and if data needs to be redacted
6. Contact anyone who uses email for business of the meeting and ask them to perform a search to see if name appears; assess how to make copies of these records

This is obviously going to be time consuming and complicated. It helps to appoint someone or a group to be in charge of responding to these requests, trying some practice attempts, and making everyone in the meeting aware that if contacted regarding such a request, there is a tight time limit for response, and co-operation is required.

*****One very important tip – do not continue to use the person's name when communicating about the request as this could create more data you have to give them copies of!! This is important to highlight in any initial communications to people helping collate the response. Refer to them as *the requestor* or suchlike. Also avoid hypothesizing about what may have led them to make such a request / past grievances etc.**

It is also worth noting that requests refer to data held by the organisation up until the date of the request, you do not have to include data created thereafter. The above advice is still sensible though, it is good practice, and there is nothing to stop a requestor making another request at a later date.***

When you have collated all the copies of information you can find, check over them all to make sure you have not inadvertently included other people's data.

You should include an explanation of the context of the data, ie. *Emails 1-12 are general circulars sent to all members; image 7 is a screengrab of our contacts database featuring your data – we use to contact people about events, we ask consent for all names to be added to this.*

(*This is explained further on the ICO page linked to at the top of this guide*).

If you have email exchanges about sensitive issues, explain the context, e.g. *Emails 4-8 concern your application for membership, and concerns Friends had around your readiness for joining the meeting*.

Do not be tempted not to hide data or amend data – this will look much worse if it is later found that it was not disclosed. Even if you decide to withhold documents from the requestor, you should tell them of their existence and explain why you are withholding them.

There may be a difficult grey area around what constitutes records of the meeting, and what constitutes personal records, particularly with email. The relationships in meetings cross boundaries between 'organisational' and 'personal'. The ICO may be able to advise if you cannot make this distinction yourself.

Second response – giving access

Hopefully you will have made a reasonable search of all records and collated the copies within one month. There are grounds to claim an extension:

The ICO gives three reasons:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- you are requesting proof of identity before considering the request.

As a volunteer organisation, with little or no paid staff, it may be reasonable for a meeting to argue they need more time as they have limited resources – if you email the requestor to explain this, hopefully they will agree. The ICO will prefer that you have kept the person informed about the extension, then if you just respond in two months' time with no explanation or communication with the requestor.

Send the formal response with the copies of the data, and metadata necessary to explain what the copies are. It is good practice to send this in the format you received the response unless the requestor has asked otherwise.

When you respond, you can be honest about what the process involved. If you say for example, "*we have made all reasonable searches within our capacity and believe this is a full copy of the records we hold with your data*", it conveys that you have made as best an attempt that you can, within your means and capacity as a small, volunteer run organisation. You perhaps cannot say *for certain* that no other data exists, but you have made fullest searches in good faith to comply with the request.

As always, somewhere in your response, you have to say that the person has the right to complain to the ICO should they be unhappy with how the response was dealt with.

Recordkeeping

As mentioned above it is important to keep a record of this entire process, from all communication with the requestor to a record of what you gave them in the same format. This is important to demonstrate to the ICO how you dealt with the request. The ICO does not have unrealistic expectations of small organisations. If you feel you dealt with the request in good faith, and to the best of your abilities, they should be satisfied (and may have advice for improving your systems).