GDPR:
Audit document

This document is part of our GDPR toolkit and is designed to help you think about the questions you need to ask about the data your group holds, asks for and uses, to help you prepare for GPDR.

Before using the tool we suggest you read our general GDPR guidance.

How the guidance works

GDPR is a meaty topic with lots of information to take on board. We do have an interactive audit tool in the GDPR toolkit that allows you to filter the information in this guidance to access the parts relevant to you based on the sort of data you hold.

We have tried to cover what we think we will be most common scenarios faced by member groups, but realise all groups are different. If you feel something is not covered please get in touch so we can a) advise you further and b) develop the tool.

Contents

Section 1 – General

A. Safe and secure storage of data

Under GDPR holding data is not a problem – the main focus is that you have good reason and/or consent to be holding and using the data. However, any good reason or consent is meaningless if that data is not stored securely. There is no huge trick or secret to safe and secure storage - it is about having common sense rules and measures in place, and following them. This should apply to physical and digital data:

- Have a well organised and clear filing system – well organised data is easier to manage and reduces risk of mis-use or loss of data. It will also make your regular review of data easier too.
- Any electronic data should be password protected. For third party sites/services this is fairly easy as they tend to come with password logins. You should also think about passwords for devices where data is stored (e.g. password to login on laptop) or the file where the data is (e.g. password-protected spreadsheet) – or both.
- Just having a password is not enough. Keep track of who has the passwords and change them regularly. Every six months as standard is a good idea but also think about doing it when people with passwords leave a role.
- The same applies for physical data, but for 'password' read 'key/combination code'. It's not uncommon for paper to be in the house of a committee member – you could argue that their house is secure so the data is secure – but ideally any data, especially sensitive data, should be kept in a locked space (draw, filing cabinet etc.). Certainly if you have some storage space at a local community building then any data should be kept locked. Keep track of who has keys or combination codes. Change codes regularly and if someone leaves a role make sure any data and keys are returned and codes updated.

Action to take

Review the data you hold:

- Who has what and where is it?
- If it is scattered about can you bring it together in fewer places?
- Once you know who has what data make a register and keep it up to date

Review security measures:

- Is data behind passwords/locked?
- Who has the passwords and keys/codes?
- When were they last updated? Do you need to change them?
- Develop some procedures around updating passwords/combination codes and collecting data when people leave.

B. Giving people in your organisation specific responsibility for data protection

Under GDPR you probably don't have to appoint any mandatory roles. Some organisation (public authorities and those processing large scale sensitive data) do have to appoint a Data Protection Officer (DPO).

Whilst it is very unlikely our groups will *have* to appoint a DPO, it is good practice to appoint someone to lead on GDPR preparations, and be in charge of how data is collected, stored and used on an ongoing basis. They should also be the contact for anyone who has a request regarding their data.

You might want to also think about appointing some other people to assist with GDPR preparations too.

Action to take

- Appoint someone to be the lead and contact on GDPR preparation and ongoing data protection. Or if you already have someone in charge of data protection make sure they are up to speed on GDPR. (If they are not registered on our site you can invite them via your dashboard so they can access our resources).
- Think about other roles to support with GDPR preparations.

Section 2 – Member data

A. Holding and asking for basic contact data on your members
(e.g. name, phone, email, postal address)

Legitimate use (Admin): By someone being a member you have a legitimate reason for keeping and using this information for membership administration purposes. This can include things like notifying of rehearsal changes, informing of performance schedule, notifications of membership fees due, AGM notification etc. This type of use is implied by them being a member and you don't need any specific permission. But you should still make them aware of how their data will be used at the point of collection.

Find out more about Legitimate interest

Marketing emails: Using contact details for other purposes, such as emailing about upcoming events and promoting the group activities, is less clear. You could argue that these activities are part of being in the group and so is legitimate use. However, they are not essential to membership – for someone who just wants to sing in your choir there is a clear practical necessity for emailing them about a rehearsal time change or because their fees are due. The same can't be said of an email promoting a quiz night – it is not essential (although may be desirable) to their membership of the choir. So for these types of communication you should have consent from the member.

Exactly how you manage this may depend on how you email:

- If you do all emailing (admin and marketing) through a mail service (e.g. Mail Chimp) they may be set up with a single opt-out option which is applied automatically. So if a member opts out you cannot override it to send an admin email.
- If you do all emailing (admin and marketing) through a normal email account (e.g. Gmail) then you will need clear lists of members opted in and out of marketing emails – and a procedure to make sure this is followed.
- The ideal situation might be to use an email service (e.g. Mail Chimp) for your marketing emails – and use personal email (e.g. Gmail) for group admin. This separates out the two areas of legitimate use and marketing emails and will make managing consent easier.

Reason: for members with contact details the distinction between admin and marketing emails and consent is perhaps the biggest challenge, but you should give some consideration to the reason for having/collecting the data. It is probably fair to keep the data but it is still worth asking the questions:

- Email – there would normally be a good clear reason
- Phone – probably a legitimate useful reason in terms of last minute changes
- Address – your constitution may state you need to keep a register of addresses in which case you have good reason. Even if it doesn't (or you don't have a constitution) you could probably argue it was good membership admin practice, if you wanted to.

Action to take:

Audit - do an audit of contact detail data you hold on existing members – do you have a good reason for asking for it and storing it?

- Yes - make sure it is stored safely and securely and include the data in your next data review to see if you still need to have it.
- No – delete the data.

Inform and get consent: think about how you will inform members of how their data will be used and get consent for marketing communications. Members are probably the easiest group to get consent from. You could have some sign-up sheets with clear privacy statements and tick boxes for types of email communication at rehearsals over the next few months for existing members.

Review the information you ask for at the point of someone new joining as a member:

- Do you have good reason for asking for it? If not, update your processes/forms so you no longer ask for it
- Do you provide a clear and simple privacy statement informing the new member of how their data will be used? If not, develop one – templates available in our GDPR toolkit soon.
- Do you ask if they would like to receive marketing emails? If so, ensure you ask for positive consent and that use is covered in your privacy statement.

Email systems:

- Think about what constitutes admin communications and marketing communications – you don't have to have a definitive list but some criteria/way of deciding might be useful.
- Think about how you will manage your email systems to ensure opt-outs are taken into account for marketing communications.

B. Holding and asking for other personal data on your members (this could be a wide range of things such as bank details, economic data, demographic or medical data)

Other personal data – the definition of personal data is quite broad and you may well hold some other types of personal data. Whether you should will depend on why you have it.

- Bank details **–** if you make a regular payment (e.g. expenses) then keeping bank details is fine. If you have a members bank details for a one-off payment then there is probably no reason for keeping these on file.
- If you offer concession subscriptions for those on benefits or low income then there may be a legitimate reason for keeping some economic data. Likewise a Gift Aid declaration form might contain some economic data.
- You may be asked to collect data about your members for a funding bid or report – does the data have to be personal or can it be anonymised? For example, it will probably be ok to say 40% of members are aged between 40 and 50, rather than keep data that can be linked to an individual person.
- Medical – you may have a list of medical conditions that you need to be aware of for rehearsals – this seems to be legitimate. But do you still have medical conditions listed for former members? There is probably no reason to keep these on file.

Action to take:

Audit: do an audit of all this type of information that you hold on existing members, and decide if you have a legitimate reason to keep it:

1. Yes - can it be anonymised? If not, make sure it is stored safely and securely and include the data in your next data review to see if you still need to have it.
2. No – delete the data.

Review the information you ask for as standard at the point of someone new joining as a member:

1. Do you have a good reason for asking for it? If not, update your processes/forms so you no longer ask for it
2. Do you provide a clear and simple privacy statement informing the new member of how their data will be used? If not, develop one (template available in our GDPR toolkit).

Where you ask for information on an ad hoc basis ensure you have a good reason for asking for it, think about if it can be anonymised at the point of collection, make it clear why you are asking for it and how it will be used.

Find out more about Personal data

C. Taking and using photo and video images of your members (e.g. website and printed marketing material)

Under GDPR photos are considered personal data. If you are going to take and use photos or video footage of individuals then you should have positive consent from them. It will no longer be sufficient to say 'photos are/video is being taken – let us know if you would rather not be photographed'.

An important thing to remember is that to be considered personal data you have to be able to identify the individual from it. So a long shot of your group on stage might be OK. But for any clearly identifiable images then you should have a positive opt-in/consent from each individual.

Action to take

The issue of positive consent for photos/video is potentially one of the trickier areas. It might be something you need to discuss and weigh the risk against what is practically possible. That said, where members are concerned it should be fairly easy to get the required consent.

Review existing photos in use and decide if the individuals in them are identifiable:

- If yes – check if you have specific consent
- If you don't, can you contact them to ask for it?
- If you can't do this, can you use a different image where you do have consent?

Decide how to approach consent for future photos/video of members

- Include photography in a privacy statement for members. You should still make people aware of when photos are being taken.
- Ensure you have a system in place to ensure images of anyone who has not given consent are not used.
- You could also treat it on a case-by-case basis. The big risk is not so much having the photos (as long as they are stored securely) as actually using them publicly. So, if you have some photos or video footage you want to use you can ask the member before using it to be absolutely clear about consent.
- Delete photos you don't need:
    - With digital photography it is common to have lots of images – try and be disciplined about deleting those you know you won't ever use as soon as you can
    - Obviously there will be some you might not want right now but are worth keeping on file. These should be stored securely and included in your regular review of data held.

Section 3 - Audience members and mailing list contact data

A. Audience members booking event tickets with you directly

Booking events: if people book event tickets through you then think about the information you collect when booking. It is fine to collect information if you have good reason for doing so. Such as:

- email address and phone number - necessary for event communication
- address - necessary to post out tickets – but if you email the tickets is postal info really necessary?

Assuming you have good reason to collect this information then you can use it for that purpose – such as event confirmation and reminder emails: However:

- You should still make it clear to them at the point of booking how the data will be used.
- You can't use the data for another purpose – such as emailing them about another event - unless you have permission to do so (see below).

Actions to take

Audit of data you currently hold on individuals who have previously booked tickets.

- Do you have a good reason to be storing the data?
    - Yes - can it be anonymised? If not, make sure it is stored safely and securely and include the data in your next data review to see if you still need to have it.
    - No – delete the data.
- Do you have consent to use the data for marketing purposes? (see Mailing list section for more details)

Review information you ask for at the point of someone booking

- Do you have good reason for asking for it? If not, update your processes/forms so you no longer ask for it.
- Do you provide a clear and simple privacy statement informing the individual of how their data will be used? If not, develop one – template available in our GDPR toolkit soon.
- Do you ask if they would like to receive marketing emails? If so, ensure you ask for positive consent and that use is covered in your privacy statement.

B. Holding and asking for basic contact data on your audience members and people on your mailing list

(E.g. name, phone, email, postal address)

Mailing lists and opt-ins

If an individual has given permission for you to keep and store their data for the purposes of promoting your activities then it is fine to do so. But that permission has to be a positive opt-in and specific to the use. It is no longer acceptable to take the 'unless you tell us otherwise' approach.

- Website: you can no longer have pre-ticked boxes for sign-up for emails – a user must actively tick a box to say they want to receive emails. The form should also be clear about what sort of email they will get and there should be easy access to a clear and simple privacy statement.
- On a paper email sign-up form – there should be a tick box to say they want to receive an email, or it should be very clearly stated that by adding their email they are agreeing to receive emails. There should also be a clear and simple privacy statement available at the point of sign-up (perhaps on the back of the form).

We know a lot of groups have a sign-up sheet along the lines of: 'sign up to enter a prize draw for free tickets – by signing up you also agree to go on our mailing list'. This is not compliant with GDPR as it is forcing mailing list opt-in as a condition of something else. There should be the choice to opt-in, or out, of both options (such as a sign-up sheet with two tick boxes). This is an area of GDPR that might seem overly regulatory and something that will hamper your group. This is an understandable point of view and it could be one of those situations where you balance the letter of the law against the spirit of GDPR and needs of your group:

- You might make the decision to carry on as you are – the sign-up sheet is very clear (they could just not enter the prize draw at all), you will use the data in a fair and reasonable way and always provide an opt-out option.
- That said having two tick boxes is not too difficult. If they are supporters of your group who want free tickets they are probably unlikely to object to emails anyway. An additional factor is the quality of your mailing list. It is not always good to force someone to opt-in if they don't want emails. It is better to not have someone at all rather that to send one email that is then marked as spam.

Reason: Finally think about what data you are collecting and if you have a reason for doing so. If you don't send anything in the post there is no reason to ask for an address. For mailing lists it is probably best to keep it as simple as possible and just ask for names and emails.

Action to take

How you collect and use data for a mailing list is probably the area that will have the biggest impact on your group.

Audit: take a full audit of all the information you hold on individuals currently on your mailing lists and decide if you have a legitimate reason to keep it. You probably need to be a bit more brutal with this group of people than with members. There are less grey areas in terms of use of data and potentially more risk.

- Yes - can it be anonymised? If not then make sure it is stored safely and securely and include the data in your next data review to see if you still need to have it.
- No – delete the data.

Review the information you ask when collecting data for your mailing list.

- Make sure you have good reason for asking for it – if you won't use it, don't ask for it.
- Ensure you provide a positive opt-in
- Provide a clear and simple privacy statement at the point of collecting the data explaining what the data will be used for.

Consent (opt-ins)

Historical opt-ins - one of the main questions around GDPR is; do you need to get positive opt-ins for people who have signed up under previous (non-positive) opt-ins? To be honest it is a bit of a grey area, and we think there is some common sense to be applied.

One option is to email everyone who you usually email/have evidence of a historical non-positive opt-in for and ask them to provide a positive opt-in:

- If you do not currently email them, or have evidence of any historical opt-in, then you should not email them asking for a new opt-in.
- If you take this approach and they do not opt-in or reply then you should not email them anymore.

You could consider splitting your contacts into two groups:

1. **Engaged:** If you have been emailing an individual about your activities for some time and you have good evidence that they engage with these emails then you could reasonably argue that you have good reason to carry on without asking for a new positive opt-in. What might this engagement look like?
    - If you use an email service like Mail Chimp you may be able to get open rate stats – if someone is opening most your emails then they are probably happy to keep getting them.
    - Regular correspondence with someone following marketing emails.
    - Regular attendance at events.

- **Not engaged:** If you have been emailing them but don't have evidence of engagement – then you should probably contact them and ask for the positive opt-in. If they don't provide it you can't email them anymore.

Opt-outs: whenever you use data provided there must be a clear and simple way for people to opt-out of future communications, and you will need a clear procedures for acting on this quickly and ensuing they don't receive any more emails.

C. Holding and asking for other personal data on your audience members and people on your mailing list

(this could be a wide range of things such as bank details, economic data, demographic or medical data)

- It is hard to see why you would need to keep details other than basic contact details for a mailing list.
- You may collect demographic data on your audience for funding bids or reporting. This could probably be anonymised. It should be ok to say 30% of attendees were under 30 rather than keep data that can be linked to in individual person.

Action to take

Audit of data you hold on individuals currently on your audience members and mailing list.

Do you have a good reason to be storing and for asking for it?

- Yes - can it be anonymised? If not, make sure it is stored safely and securely and include the data in your next data review to see if you still need to have it.
- No – delete the data.

Review information you ask for at the point of collecting data

- Do you have good reason for asking for it? If not, update your processes/forms so you no longer ask for it.
- If you collect demographic data from audience members can it be anonymous at the point of collection?

D. Taking and using photographs or video footage of your audience

Under GDPR photos and video footage are considered personal data. If you are going to take and use photos or video footage of individuals then you should have positive consent from them. It will no longer be sufficient to say 'photos are/video is being taken – let us know if you would rather not be photographed'.

An important thing to remember is that to be considered personal data you have to be able to identify the individual from it. So large audience shots might be OK, but for any clearly identifiable images then you should have a positive opt-in/consent from the individual.

Action to take

The issue of positive consent for photos/video of the audience is potentially one of the trickier areas, and may be something you need to discuss and weigh risk against what is practically possible.

Review existing photos in use and decide if the individuals in them are identifiable:

- If yes – check if you have specific consent
- If you don't, can you contact them as ask for it?
- If you can't do this, can you use a different image where you do have consent?

Decide on an approach for future events where you will be taking photos/video

- Have a sign-up sheet for the audience on arrival asking them to consent to their image being used. Include a clear and simple privacy statement. Be aware that if someone does not consent then you will have to have a way of ensuring their image is not used.
- One option might be to inform the audience that photographs are/video is being taken but that you will contact them for consent if it will be used publically. This does rely on you being able to contact the person and may restrict which photos you can use.
- Delete photos you don't need:
    - With digital photography it is common to have lots of images – try and be disciplined about deleting those you know you won't ever use as soon as you can
    - Obviously there will be some you might not want right now but are worth keeping on file. These should be stored securely and included in your regular review of data held.

Section 4 - Volunteer and freelancer data

A. Holding and asking for basic contact detail on your volunteers and freelancers?

(e.g. name, phone, email, postal address)

Legitimate use: you have a legitimate reason to store and use this data for the purposes of communicating with them about their role with your group. You should still make them aware of how their data will be used at the point of collection.

Marketing emails: to use the data for any other reason (such as promoting group activities) then you would need a positive opt-in. There is potential for some grey area here. If, for example, part of the volunteer role was to sell performance tickets then it might be legitimate to include them on a promotional emails about the event as it would be relevant to their role.

Action to take

Audit - do an audit of contact detail data you hold for existing volunteers and freelancers – do you have a good reason for keeping it?

- Yes - make sure it is stored safely and securely and include the data in your next data review to see if you still need to have it.
- No – delete the data.

Review the information you ask for at the point of someone joining as a volunteer:

- Do you have good reason for asking for it? If not, update your processes/forms so you no longer ask for it
- Do you ask if they would like to receive marketing emails? If so, ensure you ask for positive consent and that use is covered in your privacy statement.

Inform and get consent (Privacy statement): think about how you will inform volunteers and freelancers of how their data will be used and get consent for marketing emails. Design a clear and simple privacy statement for volunteers and freelancers – make sure existing and new volunteers see and agree to it.

Email systems:

- Think about what constitutes communications relating to a volunteer/freelancer role and what is marketing communication – you don't have to have a definitive list but some criteria/way of deciding might be useful.
- Think about how you will manage your email systems to ensure opt-outs are taken into account for marketing communications.

B. Holding and asking for other personal data on your volunteers and freelancers

(this could be a wide range of things such as bank details, economic data, demographic or medical data)

There could be a range of different information you hold in volunteers/freelancers. As with all GDPR data the key question to ask yourself is do you have good reason to keep it, and are you using it? Some examples might be:

- Bank details **–** if you make regular payments (e.g. fee or expenses) then keeping bank details is fine.
- You may be asked to collect data about your volunteers for a funding bid or report – does the data have to be personal or can it be anonymised? It will probably be ok to say 25% of volunteers are aged between 18 and 35, for example, rather than keep data that can be linked to in individual person.

Action to take:

Audit all information currently held on volunteers and freelancers and decide if you have legitimate reasons to keep and use this formation.

- Yes - can it be anonymised? If not then make sure it is stored safely and securely and include the data in your next data review to see if you still need to have it.
- No – delete the data.

Review the information you ask for at the point of someone joining as a volunteer/freelancer:

- Do you have good reason for asking for it? If not , update your processes/forms so you no longer ask for it
- Do you ask if they would like to receive marketing emails? If so. ensure you ask for positive consent and that use is covered in your privacy statement.

Section 4 – Data with third parties

A. Storing and using data via third parties

e.g. sharing documents (Google Drive), an email service (Mail Chimp) or an online ticketing website (Ticket Source).

GDPR applies to non-EU companies that are storing and using data of individuals within the EU. It is your responsibility to ensure any third parties you use to store data are compliant with GDPR. This does not mean you should be telling Google about GDPR, but it does mean you should do some research to make sure they are compliant. The potential area of complication is when you are using a service but the organisation delivering that service houses data outside the EU. The good news is that many of the bigger more common organisations are either based in, or have a base in, the EU and so will be up to speed with GDPR. Some smaller, less well-known organisations based outside the EU could be storing data outside the EU which makes things more complicated.

Action to take

Review all third parties you use and do some research into their GDPR awareness/compliance. Normally a quick internet search will bring up the key information you need know. If you are struggling to find any information on a third party then you may need to dig deeper to find out where they keep their data or get in touch with them. If information is hard to come by then it might be best to err on the side of caution and look for an alternative. If you, as a leisure time music group, are thinking about GDPR and they aren't, can you really be confident that the data is safe?

We will be producing a list of common third parties used by groups soon. If you come across any you use that you are struggling with finding information on please do get in touch.

National Federation of Music Societies (trading as Making Music). A company limited by guarantee. Registered in England no. 308632 Registered Charity in England no. 249219 and in Scotland no. SC038849. 8 Holyrood Street, London SE1 2EL. Tel 020 7939 6030