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 to help you meet your data protection responsibilities.

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 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.

Published February 2018
Updated May 2019

Contents

Before you start

It's useful to understand a little about 'lawful basis of processing. The key thing about data is not that you have it – but that you have a good reason to have it. You can hold and use data – but you need what's called a 'lawful basis for processing' it – basically a justification for having it.

There are several legitimate lawful reasons for having data. We think there are three that will most commonly apply to our groups.

1. Legitimate interests: if an individual asks you to do something (e.g. provide a service) you have a legitimate interest to hold and use their data as part of doing the thing they requested. In this instance you don't need specific consent – essentially the request for the service legitimises you having the data. If someone wants to join your group asking for their name and contact details for your records is a legitimate interest. As would be using these details to email them about a rehearsal change or subscription fee reminder.
2. Contract: this is similar to legitimate interests but relates to when you have a contract in place with someone and you need to use their data to meet your obligations under the contract. An example might be having your MD's contact details and bank account details so you can manage their working relationship with you and pay invoices.
3. Consent: with 'legitimate interests' and 'contract' the basis for having and using the data is implied in the activity. In some instances, this won't be the case, and you will need clear consent from an individual to use their data. This is most commonly the case where you are using the data to promote a product or service, such as an event.

How consent is given	Specific	Positive
Someone buys an event ticket and included in the terms of purchase is signing up to your e-newsletter.	X	X
Someone buys an event ticket at the bottom is a pre-ticked box that means they will sign up to your e-newsletter.	✓	X
Someone buys an event ticket – there is an un-ticked box that says if they tick it they will sign up to your e-newsletter.	✓	✓
You have a form on your website that says 'enter your email to sign-up to our mailing list' with a 'submit' button	✓	✓

Whatever your reason for holding the data you should provide the individual with a privacy statement when you collect their data. This should be short and use simple language that explains how you will use the data. It should also explain where they can find more detailed information (privacy notice).
An important point is that you might need different reasons for using the same bit of data in different ways. For example

- Holding a soloist's email so you can contact them about performing with you = contract
- Holding a soloist's email so you can tell them about all your group's events = consent

Section 1 – Member data

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

Legitimate interests (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 group. 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.

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.
- 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 can be considered personal data. An important thing to remember is that to be considered personal data you have to be able to identify the individual from it. So long shots, soft focus and backs of heads might be OK. But if a person can be clearly identified then it may be classed as personal data.

Assuming that a photo/video footage is classed as personal data the next questions is: on what grounds can you use it? Guidance here is a bit unclear.

- One interpretation is that you need consent – and under GDPR that consent would have to be positive. In which case having a sign saying ‘we are taking photos/video please let us know if you would rather not be photographed’ is not sufficient as individuals have not taken action to say ‘yes you can use a photo of me’. Practically this could be very hard to manage - especially with audience members at an event.
- Another interpretation is that the use of photos/video footage comes under legitimate interest – and therefore you don’t need consent. The argument being something along the lines of:
    - Promoting your group is necessary and a legitimate interest
    - Having photos of your activities taking place is not an unreasonable way to do this

    - The rights, interests and freedoms of any individuals in the photos/video are not at significant risk.

We think the legitimate interest interpretation is a good one. If it is used it should still come with other measures, such as:

- Letting members know when photos/videos are being taken.
- Minimise the risk of someone being identified when you do use their image publically (e.g. don't use captions like. 'Eric Bennet plays the drums')
- For close-ups of individuals you might want to ask for permission anyway as a courtesy - even if you are using it under legitimate interest.
- Store anonymously – avoid saving files using member's names where you can, and don't have it linked to any other data you might have on the individual. And, as ever, store everything safely and securely.

Find out more about legitimate interest.

Action to take

Review existing photos/videos you have and use. You can apply the legitimate interests interpretation (above) to existing promotional photographs/videos (e.g. on your website), including for people who are no longer involved in your group. You could still think about what you can do to remove risk of identification (e.g. captions). Also consider photos you store but don't actively use:

- Do you actually need them? Will you ever use them? If not delete them.
- If you do need them – are they/can they be stored anonymously?

Decide how to approach future use of photos/videos of members

- Reference photography/video footage in a privacy statement for members.
- Whilst you might not need consent you should still make people aware of when photos/videos are actually being taken.
- Think about your approach to how you take and publically use photos/video to minimise risk:
    - Take photos in a way that means people are not identifiable - long shots, soft focus, angles etc.
    - If an individual is identifiable don't include any data that may increase the risk (e.g. captions)
- Delete photos you don't need:

D. Asking for and holding personal data on children in your membership

If you have children in your membership then you can probably treat their data in the same way as an adult's data in terms of where you do, and don't need, consent to collect and use their data. The key difference is that if the child is under 13 whoever has parental

responsibility for the child should see privacy statements and give consent. Children over 13 can give their own consent. This includes when a child who is an existing member has their 13th birthday, in which case you should get new consent directly from them.

Under GDPR children have the same rights over their data as adults and whilst fair and responsible use of all data is important, extra emphasis is placed on children's data

Action to take

Audit: do an audit of any data you hold on children in your existing membership, and decide if you have a legitimate reason to keep 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 the information you ask for as standard at the point of a child joining as a member:

- Do you have a good reason for asking for it? If not, update your processes/forms so you no longer ask for it
- Do you speak with whoever has parental responsibility for the child to:
    - provide a clear and simple privacy statement informing them how the child's data will be used? If not, develop one – templates are available in our GDPR toolkit soon.
    - ask if they would like the child to receive marketing emails? If so, ensure you ask for positive consent and that use is covered in your privacy statement.
- If the person with parental responsibility would prefer to receive emails on behalf of the child have a mechanism for this (e.g. getting consent)
- Have a process for getting consent from the child once they turn 13.

Section 2 - 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 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 data than with your member list. 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 for 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.

If you have been sending promotional emails to people about events for years but don't have evidence of if/when they opted-in – you don't need to email them and ask them to opt-in now. The fact that you have been emailing them for years and they have not objected is consent enough. Of course, for any new data you collect for your mailing list you must get consent.

Opt-outs: whenever you send an email to your mailing list you must provide be a clear and simple way for people to opt-out of future communications. You will need a clear procedure 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 can be considered personal data. An important thing to remember is that to be considered personal data you have to be able to identify the individual from it. So

long shots, soft focus and backs of heads might be OK. But if a person can be clearly identified then it may be classed as personal data.

Assuming a photo/video footage is classed as personal data the next questions is: on what grounds can you use it? Guidance here is a bit unclear.

- One interpretation is that you need consent – and under GDPR that consent would have to be positive. In which case having a sign saying 'we are taking photos/video please let us know if you would rather not be photographed' is not sufficient as individuals have not taken action to say 'yes you can use a photo of me'. Practically this could be very hard to manage - especially with audience members at an event.
- Another interpretation is that the use of photos/video footage comes under legitimate interest – and therefore you don't need consent. The argument being something along the lines of
    - Promoting your group is necessary and a legitimate interest
    - Having photos of your activates taking place is not an unreasonable way to do this
    - The rights, interests and freedoms of any individuals in the photos/video are not at significant risk.

We think the legitimate interest interpretation is a good one. If it is used it should still come with other measures, such as:

- Always telling audience members that photos/video footage is being taken (.e.g. large signs and announcements)
- Minimise the risk of someone being identified when you do use their image publically (e.g. don't use captions like 'Brenda Bennet enjoys our performance of…')
- For close-ups of individuals you might want to ask for permission anyway as a courtesy - even if you are using it under legitimate interest.
- Store anonymously – avoid saving files using member's names where you can, and don't have it linked to any other data you might have on the individual. And, as ever, store everything safely and securely.

Find out more about legitimate interest.

Action to take

Review existing photos/videos you have and use. You can apply the legitimate interests interpretation (above) to existing promotional photographs/videos, (e.g. on your website). You could still think about what you can do to remove risk of identification (e.g. captions). Also consider photos you store but don't actively use:

- Do you actually need them? Will you ever use them? If not delete them.
- If you do need them – are they/can they be stored anonymously?

Decide how to approach future use of photos/videos

- If you are taking photos/video footage at an event make it clear to audience members that you are doing so. You should also make sure people have an easy way to

discuss it with you. If someone is insistent that they do not want their image used then you shouldn't use it. There are a few ways this could be managed:
    - Make a note of where they are sitting and try and exclude them from photos/footage.
    - Take a head shot/image to use as a reference and don't keep photos/footage of them that you do take.
- Think about your approach to how you take and publically use photos/video to minimise risk:
    - Take photos in a way that means people are not identifiable - long shots, soft focus, angles etc.
    - If an individual is identifiable don't include any data that may increase the risk (e.g. captions).
- 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: anonymised (where possible), stored securely and included in your regular review of data held.

Section 3 - Volunteer and freelancer data

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

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

Contract: you have a legitimate reason to store and use this data for the purposes of communicating with them about their role with your group and fulfilling your part of a contract/agreement. 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.

Disclaimer:

We hope you find this Making Music resource useful. If you have any comments or suggestions about the guidance, please contact us. Whilst every effort is made to ensure that the content of this guidance is accurate and up to date, Making Music do not warrant, nor accept any liability or responsibility for the completeness or accuracy of the content, or for any loss which may arise from reliance on the information contained in it.