General Data Protection Regulation (GDPR) and Individual OA Meetings

What is GDPR?

It might be easiest to think about the GDPR as European Union (EU) regulations relating to privacy laws, or anonymity guidelines. The General Data Protection Regulation (GDPR) is a mechanism by which the EU intend to strengthen and unify data protection for all individuals within its jurisdiction. These new laws are very detailed, and they apply to all organisations (including OA) across the globe handling personal information about its members who are based in the EU. These new regulations will come into effect from May 25th 2018.

What is 'Personal Data'?

Personal data is the legal term used to refer to any information that identifies a living person, like their name, email address, telephone number, photograph, etc. 'Name' includes first names if they are accompanied by a telephone number, an email or physical address or a photograph.

Does your meeting need to take any action?

YES.

If your meeting takes place in a European Union country, or the UK, the GDPR ("anonymity laws") will definitely apply to you. If your meeting is in another country in Region 9, we urge you to check your local data protection laws to make sure you are compliant.

Further on in this document there are certain actions which need to be taken, and these actions need to be documented.

What is a data breach?

One example of a personal data breach is when an unauthorised person has received access to personal information of an OA member. Another example is if we lose personal data (contact info, etc) that we are supposed to protect.

Examples include:

- access by an unauthorised third party (eg - family member sharing a computer where this information is stored);
- sending personal data to an incorrect (email, text message, etc) recipient;
- personal data being lost or stolen (phone stolen, flash drive lost);
- alteration of personal data without permission; and
- loss of availability of personal data.

What you need to do <u>NOW</u>

To help local OA meetings prepare for the introduction of these new regulations, the R9 GDPR Committee has compiled the following guidelines, accompanied by examples of suggested meeting Group Conscience decisions which can be edited to suit individual groups. <u>It is important that your group conscience develops a check system to ensure that the policies are adhered to.</u>

What will happen if no action is taken?

If there is a data breach by a meeting there is a legal obligation by the organisation concerned to notify the necessary government office (in the UK this is the "Information Commissioners Office") within 72 hours. Intergroups and National Service Boards throughout Region 9 will have to set up a system of reporting these breaches, should they occur.

Note, the Intergroup, NSB, Region 9 and the World Service Office of OA are not responsible for the compliance of individual meetings. Neither are they responsible for reporting any data breaches.

Guidance/Suggestions to assist in GDPR compliance for individual OA groups

Identify who will be responsible for data protection within the group.

There should be a clear point of contact for members who want to raise a data protection query or issue. This should be one person, e.g. the secretary of the meeting.

Meeting listing on oa.org

OA Inc is a US organisation and as such falls outside the scope of GDPR. However, they will be handling personal information about individuals and meetings that take place in Europe. The R9 GDPR committee are in communication with the World Service Office (WSO), and more information about this will be supplied when it becomes available.

Personal information required when listing a meeting, is the name and contact details of the meeting secretary, and the name and contact details of the person editing the information. Optional is a meeting contact name and number.

There are four issues that your meeting needs to consider:

1. The name and contact details of your meeting contact will be in the Public Domain. The member concerned needs to be aware of this and give permission for their details to be published on oa.org
2. The name and contact details of the meeting secretary will be held securely by WSO. This data will not in the Public Domain but may be passed to Service Body representatives within OA.
3. It is a legal requirement that the information held by WSO is accurate to the best of their ability.
4. The meeting should take a group conscience decision to ensure the meeting contact details are always up to date.

Flyers and Public Information

Event flyers/booking forms or Public Information posters often include a contact name and phone number or personal email address.

It is important that this new regulation does not prevent those struggling with an eating disorder from attending meetings/events or finding out how OA can help them. It is therefore not suggested that this practice be discontinued, rather that the member who has given their details be aware of how this data will be used and when it will be securely deleted from both the public domain and other places.

Meeting email addresses

It is strongly suggested that at least one generic meeting email address be created for each meeting. This would pass from member to member as service positions are rotated. You might find help for this from your local Intergroup or National Service Board. This will minimise the use of personal email addresses either inside or outside of OA.

If any meetings already have a generic email address, then an audit of its inbox will need to be carried out. Please see the last paragraph of 'Email listings' below.

Contact lists

Most meetings or OA events use some kind of contact list. Keeping in touch with each other between meetings is important for our recovery, but if these lists are to continue then they must be made secure.

Suggestions as to how to do this are:

- Securely destroy the daily contact list after every meeting
- Securely destroy historical contact lists
- Do not allow photographs of the page
- Inform members how their personal information will be used, and for how long it will be kept, this could be in a notice stuck to the inside of the contact list book

'Securely destroy' means to shred. Tearing the list in half or scrunching up the page and throwing it away is not sufficient.

Meeting WhatsApp groups

Some meetings have established a WhatsApp group of its members to provide support and encouragement, or communication, between Face to Face meetings.

If you do use a WhatsApp or other digital app for your group contacts, the process needs to be clear on how someone can join, and how they leave (see GC suggestions at the end of this document). There should be an identified administrator responsible for the WhatsApp group. No-one should be added to a group without their consent, and they should be removed from the group as soon as this is requested.

Email listings

A few meetings have a member email listing through which OA announcements, details of Group Conscience meetings and other such Fellowship related matters are distributed.

If you do use an email list for the group, members should give their explicit consent to join. Members should be removed as soon as they ask to be. The group conscience should make a specific decision about this process. It needs to include an assurance that email addresses will only be used for the above purpose and that they will not be communicated to third parties or other group members without the specific consent of the member.

In addition, each email account that has been handling personal information on behalf of the group needs to be audited. Any emails which are no longer required to carry out the effective functioning of the meeting should be deleted. Groups must then draw up an email policy that sets out how email is handled going forwards – how any attached documents that need to be kept are stored; how long emails are kept before deletion, for example.

Meeting records

Records of meetings held, attendance numbers, group conscience minutes, financial matters etc should not contain any personal data other than first names. Note that invoices for OA literature

may contain contact information for the member who ordered it. They should therefore be either securely destroyed once the meeting treasurer has dealt with the monies owed or stored behind lock and key, or stored digitally with a regularly changed password.

It is suggested that each meeting check their meeting materials (papers, etc) and destroy any documents containing personal data other than current event flyers.

Similarly, individual members who have been involved with event organisation or have held the Intergroup Representative service position may have personal data held on email accounts, laptops, phones, memory sticks, Dropbox etc. Delete anything that is not current and/or serving a useful purpose.

Workshops and retreats

Events such as these will attract attendees who may need to divulge personal data to book a place or share contact information. It must be made clear to them how this information will be used and how long it will be kept for.

Online/WhatsApp/Skype/Telephone meetings

These are becoming increasingly popular. It is vital that on the joining of (or participation in) any of these meetings our members are assured of personal data security, what they are consenting to their details being used for, how long the information will be retained and how they may withdraw their consent.

Meeting policies will vary depending on the medium being used and further guidance will be issued as it becomes available.

A separate guideline document will be prepared specially for these virtual meetings.

Group Conscience decision <u>suggestions</u> (these decisions should be documented in a GC notebook with the date noted):

1. We, as a group, agree to comply with data protection regulations to the best of our ability.
2. For our group, _____ will be the contact person for all things related to data protection.
3. For our group, _____ will be our contact for anyone outside of our group. _____ understands that their phone number and/or email may be published on OA websites in our country and abroad.
4. We agree that all old copies of our contact lists will now be securely destroyed. **<u>OR</u>** We agree to keep copies of contact lists for one year, secured in a locked cupboard.
5. We agree, that at the end of each meeting/once a year the contact list will be securely destroyed.
6. The meeting format should be edited to notify all members who the GDPR contact person is for the group, and how often the contact list will be destroyed.
7. We agree that nobody in the group will give anyone else's phone number or email address to a 3rd party without their prior agreement.
8. Consider whether or not to allow photographs of the contact list. Smart phones can be synced to several locations, which may mean the information is shared unintentionally. (If photography is permitted, then any reference in the contact list to OA, or how members are feeling, might no longer be thought appropriate by your meeting).