General Data Protection Regulation (GDPR) and Individual OA Meetings

What is GDPR?

The General Data Protection Regulation (GDPR) is a mechanism by which the European Union intend to strengthen and unify data protection for all individuals within its jurisdiction. It is a comprehensive updating of the rules on data protection and applies to all organisations processing personal data, including non-profits and membership organisations.

What is 'Personal Data'?

Personal data is anything relating to an identified or identifiable living person. For example, name, email address, telephone number, photograph. 'Name' includes forenames if they are accompanied by a telephone number, an email/physical address or a photograph.

Does your meeting need to take any action?

YES.

OA is a non-profit, membership organisation and as such falls within the remit of the regulation. Internationally, nationally and locally ALL OA MEETINGS AND SERVICE BODIES MUST EACH COMPLY WITH GDPR. More than that, they need to be able to demonstrate that compliance through documented policies and procedures.

What will happen if no action is taken?

If there is a data breach by a meeting after May 25th 2018, it is likely that there will be a legal obligation by the organization concerned to notify the Information Commissioners Office within 72 hours. OA South and East Intergroup, OAGB, 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.

What is a data breach?

A personal data breach can be broadly defined as an incident that has affected the confidentiality, integrity or availability of personal data. There will be a breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Examples include:

- access by an unauthorised third party;
- sending personal data to an incorrect recipient;
- personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

What you need to do NOW

To help local OA meetings prepare for the introduction of this new law, the GDPR Committee formed by SEEIG has compiled the following guidance, accompanied by examples of suggested meeting policies which can be edited to suit individual groups. It is important that your group develops a check system to ensure that the policies are adhered to.

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

Meeting listing on oa.org

OA Inc is a US organisation and as such falls outside the scope of GDPR. However, they will be processing data from individuals and meetings resident in the Europe and SEEIG need to ensure that they are compliant with the American equivalent of European law. Meetings will be notified once we are confident that data sent to WSO will be handled securely.

Personal data mandatory for a meeting listing is the name and contact details of the meeting secretary, as are the details of any person who subsequently edits the information held. 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 and/or a data processor. 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 data held by WSO is accurate to the best of their ability.
4. A meeting policy covering the above will need to be written and safeguards put in place to ensure all details are current.

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 internal databases.

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. One might be held by the meeting Intergroup rep (for example, igrepbeaconsfieldoa@gmail.com) to which all IG related information and announcements can be sent by the IG Executive Secretary. Another might be held by a member willing to answer questions about their meeting or any event that might be being hosted. For example, infobeaconsfieldoa@gmail.com 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.

'We Care' books and lists

Most meetings or OA events use one of the above. Keeping in touch with each other between meetings is important for our recovery, but if We Care documents are to continue then they must be made secure.

Suggestions as to how to do this are:

- Securely destroy the We Care page after every meeting
- Securely destroy historical We Care records
- Consider whether or not to allow photographs of the page. 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 We Care book to OA or how members are feeling might no longer be thought appropriate by your meeting
- A privacy notice will need to be seen by at the time members enter their details into the book / list. A suggested wording is in the Meeting Policy guidance. The notice could be mounted on the inside cover of the book / folder so that it is clearly on view

'Securely destroy' means to shred or Tear into very small pieces.

Meeting WhatsApp groups

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

A policy needs to be put in place surrounding the consent and withdrawing of consent for members names and phone numbers to be added to these groups. 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.

A policy should be drawn up surrounding the consent and withdrawing of consent for members names and email addresses to be added to these listings. It needs to include an assurance that email addresses will be used for the above purpose only and that they will not be communicated (either by accident or design) to third parties or other group members without the specific consent of the relevant party.

In addition, each email account that has been handling personal data 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 retained 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 will 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/regularly changed digital password.

It is suggested that each meeting audit their meeting box 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 IG 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 We Care 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.

If you have any questions regarding this document, please contact the chair at chair@oasouthandeastengland.org.uk