APPENDIX B
(Last updated 20.05.2021)

Region 9 Data Protection, Information Security, and Privacy Policies

Region 9 of Overeaters Anonymous (R9) upholds our 12th Tradition of anonymity, and is committed to protecting the privacy of everyone who shares their personal information with us.

Scope of this policy

R9 will process personal data of OA members and non-members. Individuals may subscribe to the newsletter, members may attend R9 meetings, and may act as Officers for R9. Registers will be kept of meetings, and contact details saved to email accounts. If members arrange events or workshops and produce publicity material then this will be distributed and published to the website. R9 oversees an annual Assembly which is hosted by the national OA fellowship of the country where the Assembly takes place.
R9 is committed to upholding the privacy of individuals whose personal information is being processed, and this policy describes how this commitment will be met. It applies to R9 officers, representatives, and OA members who deal with personal data on behalf of R9 or in connection with R9 (including service bodies which host R9 events).
This policy should be read in conjunction with the Data Protection Policy and the Information Security Policy.

General principles

R9 takes full responsibility for the personal information we process. Privacy will be protected, and personal information never disclosed, unless with explicit consent, or where this is to a data processor (like Dropbox, or our website hosts) or where this is required by law. We will only use personal data for the purpose which it was disclosed, and securely delete / destroy it once it is no longer required.

R9 Officers, Subcommittee members, Trustees and Representatives

OA members giving service to R9 in any of these positions will supply their contact details to R9 so that they can be contacted in order to fulfil their role within OA. If their contact details change they should notify the Chair of R9 (chair@oaregion9.org) so that the records can be updated.
The details of the officers / representatives will be held on record for the period stated in the table below. If they have signed a register of attendance at meetings then this record will be kept as below. Details will not be shared with third parties, save that email addresses will (in the course of their use) be shared with email providers, and information will be held on Dropbox.
If any officer or representative would like to object to the processing of their data, or request that processing be restricted, they should do so in writing to the Chair of R9.

Sponsor lists, Translation Lists

R9 maintains lists of individuals who have agreed to act as sponsors / provide 12 step outreach or provide translation of documents. Other similar lists may be generated at times. Consent will be sought and obtained from people named on the list, who may have their information removed at any time.

Assembly / Convention attendees

Individuals are required to register in advance of attending the R9 Assembly / Convention, and at that point they will be provided with a privacy notice which explains who will hold their data and how it will be processed. The period for which data will be retained is set out in the table below. Different principles apply to those attending in a personal capacity as compared with those who are attending in a service position.

Group representatives (information received from WSO)

OA World Service Organisation holds a register for OA meetings globally. Local groups and service bodies are required to provide contact details to this register. This data is then shared by WSO to R9 so that R9 can reach out to representatives within the area covered by the Region. This may include full names (if given to WSO), home address, email address and telephone number. If any individual wishes to be removed from the list held by WSO then they will need to contact WSO directly. They can contact R9 to have their details deleted from the R9 records.

Events flyers

OA members sometimes supply their contact details in flyers and promotional material for events and workshops. The flyers supplied to R9 for this purpose will be published on the website. A record will be kept of what information is provided. Once the event has passed then the flyer will be removed from the website.
If the OA member wishes to have the flyer removed prior to the event then they should contact the Chair of R9 who will direct the Website Officer to ensure that the flyer is removed.

Data subject rights

Under the GDPR, data subjects (people whose data is being processed), have several rights:

a) The right to know what data has been collected about them, and how such data has been processed
b) The right to make changes to inaccurate data
c) The right to withdraw consent to data processing
d) The right to ask for data to be deleted
e) The right to object to data processing, or for it to be restricted
f) The right to data portability (this only applies to automated processing, which does not happen in the context of R9)
g) The right to complain to the Information Commissioners Office

If you would like to exercise any of these rights then please contact the Chair of R9.

Consent to share information outside EU

Region 9 covers a wide geographical area, extending beyond the EU to include countries and territories in Africa, the Middle East and Western Asia. This means that R9 officers and service bodies based outside the EU may receive personal data via R9. Some may have data protection policies akin to the GDPR and others may not. In these circumstances the GDPR requires specific consent to be obtained from data subjects in order to permit their personal data to be processed. Such consent will be sought.

Right to access information

Individuals have the right to access any personal data that relates to them which R9 holds, and to be given the following information:

- The reason why the data is held
- The source of the data (if not directly from the individual themselves)
- Whether it has been disclosed to anyone else, and if so, who
- How long it will be stored
- The right to request that the data be updated, or deleted, or processing restricted in any way
- The right to lodge a complaint to the Information Commissioners Office
- Whether any automated decision-making was used to process the data
- Whether the information has been shared outside the EU and if so the mechanisms in place to protect data

This is called a 'subject access request'. Any person who wishes to exercise this right should contact the Chair of R9 via email (chair@oaregion9.org). The information should be provided within 30 days, without charge. The Chair will always verify the identity of anyone making a subject access request before handing over any information.

Process for subject access requests

Any subject access requests should be forwarded to the Chair of R9, who should record them in the SAR template.

The individual making the request should be contacted and their identity confirmed, if necessary by a telephone conversation, or by being asked to supply written evidence of their identity.

The Chair should collaborate with other Officers to identify all information which is held concerning the subject. OA does not collect a great deal of personal data, and so it is likely that the information will be limited to their inclusion on a list, register of attendance at meetings, and their subscription to the newsletter, however if the person has been an officer or R9 representative or trustee then there may be more information, including emails from them and concerning them.

All material should be reviewed and an assessment made of whether it can be immediately disclosed, or whether disclosure may adversely affect the rights and freedoms of another individual. Information about a third party should not be disclosed, and this can be edited out of documents.

Nothing should be disclosed that might prejudice a legal investigation, or where disclosure would breach some other legal duty. Specialist advice should be sought if there is any concern about whether disclosure should not be made.

The general rule is that material should be disclosed within 30 days of the request being made, although if it will take longer to prepare the disclosure then the subject should be contacted within 30 days, and informed of the delay and likely timescale for disclosure. Disclosure must be made within 90 days of the request.

If no information is held about the data subject then they should be informed.

If information is held but no disclosure is made then the data subject should be informed that no action will be taken on their request, and that they have the right to complain to the ICO.

A brief description of the disclosure should be recorded in the SAR template, together with the timing of any disclosure, and any non-disclosed material, with reasons given for non-disclosure.

Archiving and retention

Personal data should only be stored for the minimum period necessary, consistent with the purpose for which it was processed. Once the retention period has elapsed it is the responsibility of the person controlling the data to delete it. Officers are responsible for managing their own Dropbox folders and email accounts, and R9 representatives responsible for their group's email addresses.

Description of data	**Period to keep**
Contact details for R9 Officers (including sub-committees)	1 year after leaving office
Register of R9 meeting attendance	1 year after attend meeting
Emails	1 year after email received or sent

Description of data	Period to keep
Financial records (including emails)	6 years after end of financial year to which they relate
Events agenda packs	6 years after event, to enable follow up and accountability, including financial accountability
Dropbox folder contents	Officer access to Dropbox deleted by Dropbox Admin once handover period finished Contents of folders deleted in accordance with this table
Sponsor List / Translations List (or similar)	Whilst consent is in place
Assembly / Convention attendees (personal capacity *)	Four months after attendance (to provide follow up material) *Fellows who are not officers and reps
Assembly Representative (service position)	Data will be kept for 2 years and 3 months after the assembly attended.
Data for local groups and service bodies received from WSO	This data is updated from WSO on a quarterly basis
Newsletter subscribers	Whilst consent is in place

Version

This policy was drafted on 5th May 2020, and approved by R9 on [INSERT DATE].
Any questions about this policy or any queries concerning data protection matters should be raised with the Chair of R9 (chair@oaregion9.org)

2. Data Protection Policy

Region 9 of Overeaters Anonymous is committed to protecting the rights and freedoms of all individuals in relation to the processing of their personal data and provides the Data Protection policy for everyone to follow.

Scope of this policy

R9 needs to collect and keep certain types of information about the people with whom it deals. This includes OA members, subcommittee officers, trustees, R9 officers, and group representatives. It needs to process this information for a variety of reasons, such as to record who has attended meetings, distribute a newsletter, and share contact details for members who provide translations.

OA needs to comply with the General Data Protection Regulation (and current UK Data Protection Act) when processing this kind of information. To ensure this happens, we have developed this policy which sets out the obligations of R9 Officers, OA members, trustees, R9 representatives and subcommittee officers.

This policy and the GDPR apply to all personal information handled by R9, both that held in paper files and data held electronically. So long as the processing of the data is carried out for R9 purposes, it also applies regardless of where data is held, (for example, it covers data held on shared Dropbox folders and on mobile devices such as mobile phones or laptops) and regardless of who owns the PC/device on which it is stored.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Definitions

Processing

'Processing' data is widely defined and includes every plausible form of action that could be taken in relation to the data such as obtaining, recording, keeping, or using it in any way; sharing or disclosing it; erasing and destroying it.

Personal data

Data which relates to a living individual who can be identified from that data or from that data and other information which may be in the possession of the person who has access to the data.

Examples of personal data are the name and address of an OA member, and their email address or telephone number. This sort of information is often gathered by R9, for example by taking a register of attenders at Assembly, holding a list of subscribers to the newsletter, collating a list of OA representatives for an area, managing subcommittees or sharing the contact details of a member who is on a sponsor list.

Sensitive personal data

Personal data consisting of information relating to:

- race or ethnic origin of the data subject
- their political opinions
- their religious beliefs or other beliefs of a similar nature
- whether they are a member of a trade union
- their genetic or biometric data
- their physical or mental health or condition
- their sexual life
- any commission or alleged commission by them of any offence
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

R9 will rarely have access to sensitive data, save for the fact that any member of OA has, by reason of declaring their membership, shared information about their physical or mental health or condition.

Particular care should be taken in processing sensitive data.

GDPR data protection principles

Anyone using personal data must comply with the six Data Protection Principles set out in Article 5 of the GDPR as they define how personal data can be legally processed. In summary these state that personal data shall:

- Be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
- Be collected for specified explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
- Be accurate and kept up to date ('accuracy').
- Not be kept for any longer than is necessary ('storage limitation').

- Be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures ('integrity and confidentiality').

Consent to share information outside EU

Region 9 covers a wide geographical area, extending beyond the EU to include countries and territories in Africa, the Middle East and Western Asia. This means that R9 officers and service bodies based outside the EU may receive personal data via R9. Some may have data protection policies akin to the GDPR and others may not. In these circumstances the GDPR requires specific consent to be obtained from data subjects in order to permit their personal data to be processed. Such consent will be sought.

Responsibilities of R9 Officers, Trustees and Members

Officers have the responsibility of carrying out the work of R9, as directed by the Assembly, and in accordance with Bylaws and the Policy Manual. This will involve the processing of personal data. Other OA members may carry out service which will require them to process personal data, and may also have access to personal data when attending meetings, or participating in the work of R9.

All OA members must:

- Be mindful of the fact that individuals have the right to see their 'personal data' if they ask to see it. They should not therefore record comments or other data about individuals which they would not be comfortable in the individual seeing, either in emails or elsewhere.
- Immediately report the matter to the R9 Chair, if they find any lost or discarded data which they believe contains personal data, (for example, may include a memory stick).
- Immediately report the matter to the R9 Chair, if they become aware that personal data has been accidentally lost or stolen or inadvertently disclosed (for example, if their laptop is stolen or their phone is lost and it has personal data stored on it),
- Hold the contents of any personal data which comes into their possession securely.
- Ensure that any personal data they record or provide to R9 (for example, their contact details as a meeting representative) is accurate.
- Notify the Chair promptly of any changes to their personal data (for example, change of address or email address, or end of service position).
- Only ever obtain or use personal data relating to third parties for approved OA purposes.

R9 Officers must:

Ensure that they only ever process personal data in accordance with requirements of the GDPR and in particular follow the six Principles it contains. The key requirements are:

- Fair processing – for example, ensure that the individual consents to their data being used and knows what it will be used for, and ensure that it is not subsequently used for something else
- Data Security – ensure any personal data which is held is always kept and disposed of securely, (taking into account any cyber security considerations). The information security policy should be followed.
- Non-disclosure – ensure personal data is not disclosed to any authorised third party.

Familiarise themselves with this guidance and other data protection policies in the policy document and follow them at all times..
Be mindful of the scope of Data Protection regulation. This includes that fact that 'personal data' is widely defined, (and so will cover for example comments made about an individual in an email to someone else), and the fact that it covers data held on remote devices (such as tablets and on mobile phones) regardless of who owns the actual device and where the device is stored.
Seek advice whenever a new or novel form of processing personal data is contemplated or if any data protection related concerns ever arise.

Prohibited activities

The following activities are strictly prohibited:

- using data obtained for one purpose for another supplemental purpose (for example, using contact details provided for meeting attendance purposes for marketing purposes)
- disclosing personal data to a third person outside of R9 without the consent of the data subject, save where this is required by law, in which case the data subject will be informed prior to disclosure, unless this is prohibited, or proves impossible (e.g. where contact details are not available or are not working).

Implications of breaching this policy

It is a policy requirement that R9 officers will abide by this data protection policy. Any breach of this policy will be considered to be a serious matter, and may result in an officer being removed from their position. A serious breach of the Data Protection Act may also result in R9 and/or the individual being liable for civil penalties and criminal proceedings.
Also, OA is a 12-step fellowship, and so any unauthorised disclosure of personal data would also stand outside our 12th tradition of anonymity. This may be very damaging to fellows, and also undermines the fellowship and so limits our ability to carry the message of recovery.

Version

This policy was drafted on 5th May 2020, and approved by R9 on [INSERT DATE].
Any questions about this policy or any queries concerning data protection matters should be raised with the Chair of R9 (chair@oaregion9.org)

3. Information Security Policy

The sixth data protection principle requires that organisations employ appropriate technological and organisational measures to ensure the security of personal data. In this policy Region 9 has set out the processes which must be followed to keep data secure (organisational measures), and the technological measures which must be adopted.

Scope of this policy

This policy applies to everyone who processes personal data from or on behalf of Region 9. This includes R9 officers, IG, NSB and LSB Reps, Committee Chairs, service coordinators, annual Assembly and Convention hosts, and OA members. All are responsible for ensuring that if they deal with any personal data, it is kept securely and is not disclosed (either orally or in writing or accidentally) to any unauthorised third party.

General principles

OA is an anonymous fellowship, and our 12th Tradition states that: “Anonymity is the spiritual foundation of all these Traditions, ever reminding us to place principles before personalities”. We hold information about other fellows in confidence. This policy upholds the 12th Tradition. Personal information must not be shared informally, nor disclosed to people who are not authorised to see it. Data must be kept secure, and if it is no longer required, it must be securely deleted or destroyed. If data is lost or stolen then this must be reported as soon as this is realised, following the procedure in this document. Particular care must be taken when data is transferred from one place to another to ensure that it is not lost in transit.

Hard copy documents

When personal data is stored on paper (for example: a register of meeting attenders), it must be kept in a secure place where unauthorised people cannot see it.
When not required, paper or files must be kept in a locked drawer or filing cabinet.
Printouts must not be left where unauthorised people could see them, like on a printer, or on the kitchen table.
Paper copies must be securely shredded or burned when no longer required. Tearing or screwing up paper is not a secure means of disposal.
Assembly attendance lists should be destroyed each year, in accordance with the Privacy Policy .

Electronic data

Computers and devices used to access personal data must have current software installed, as legacy software is not supported by security patching. Security updates should be installed.
Devices should always anti-virus / anti-malware software installed, and kept updated.
Strong passwords must be used to secure electronic devices and also services used to access data (email, dropbox, Microsoft account etc). Passwords must not be reused, shared, saved to file, or saved to non-secure password key chains or browsers. Password management software should ideally be used, and protected with a strong password. Guidance on choosing and using passwords can be found here.
If using a shared computer, password protected services must be closed down when work is finished. Files and folders must not be left open, and the screen must be locked when away from it.
Home Wi-Fi must be encrypted to the highest standard available (ideally WPA2). Suggestions for securing home Wi-Fi are:

- Change your router admin username and password so that they are not the standard for your router.
- Change the broadcast name for your Wi-Fi (the SSID) so that it does not describe the router.
- Activate firewalls and turn off guest networks.
- Keep firmware updated.
- Unless your router is locked away, turn off WPS (the one-push button to connect to your router).

Open Wi-Fi networks must not be used to access personal data.

Mobile devices

Particular care must be taken to keep mobile devices secure: they must be password protected, and ideally encrypted. Unencrypted USB devices are especially insecure as they are so easy to lose. Ideally devices should have remote wiping agents installed so that they can be erased if stolen.

Dropbox

R9 officers make use of Dropbox (basic) to save information. Two-step verification must be activated, and a strong password used.
Documents must be saved in the correct location as per the template, and multiple copies of the same documents not allowed to proliferate. Any document which contains personal data must be saved using a filename with the suffix PD, for example: 'Website Invoices (PD)'. Each officer is responsible for their own Dropbox folder.
Documents must be deleted in line with the archiving and retention rules set out in the Privacy Policy.
The R9 Chair is the Dropbox Administrator. They will manage access to Dropbox folders, ensuring that access is only granted to current Officers, and outgoing Officers conducting a handover. Once an Officer has completed their handover then they will be removed from shared folders, and synced copies of information removed from their personal Dropbox by the Administrator.

Email

R9 Board members, Committee Chairs and service coordinators will use R9 alias email accounts for their R9 OA business, hosted by Koumbit.
Email is not inherently secure. Most emails transmitted over the internet are sent in plain text, which makes them vulnerable to interception. Consider what information is sent via email.
It is strongly suggested that generic email addresses are used wherever possible, at all levels of OA service in Region 9.At least one generic meeting email address should be created for each OA meeting, and for each IG/NSB/LSB officer and service coordinator. This would pass from member to member as service positions are rotated. One might be held by the meeting Intergroup rep (for example, IGRep-Tue-meeting@gmail.com) to which all IG related information and announcements can be sent by the IG 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, info-Tue-meeting@gmail.com This will minimise the use of personal email addresses either inside or outside of OA.
Email accounts must be securely password protected, and security features not disabled.
Great care should be taken when opening email attachments, in case they contain a virus, Trojan, spyware or other malware. It is now commonplace for ransomware attacks to be launched by 'spoof' emails which appear to come from a legitimate organisation (for example HMRC) attaching an invoice or order form, which, if opened, installs malware which encrypts all data on the attacked device. A ransom is then charged for the decryption key. Under the GDPR corruption of data is a data breach, and therefore a ransomware attack should be reported as such to the R9 Chair, as per the policy below.
When sending emails to a list, the email must be addressed in the 'To' field back to the sender, with the recipients listed in the 'BCC' (blind carbon copy) field. This means that email addresses are not shared between the whole list.
Documents containing personal data may be attached to emails, either sent or received. These must be saved securely. The emails with the attachments must also be kept secure, and

themselves deleted in accordance with the archiving and retention rules set out in the Privacy Policy.

Data breach

Reporting to R9 Chair

The GDPR requires that OA notify the relevant national authority if there is a data breach, without undue delay, and not later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of data subjects. R9 have chosen the UK Information Commissioners Office as our relevant national authority.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This might include loss of a USB stick with OA members' contact details, or accidental email of contact details to anyone not authorised to receive them.

Anyone handling personal data in connection with OA (R9 Board members, Committee Chairs, service coordinators and Reps) must notify the R9 Chair as soon as they become award of a data breach (chair@oaregion9.org). Anyone who has concerns about data privacy or the risk of a breach should notify the Chair of their concerns.

Notification to ICO

The Chair will consider whether the breach is likely to result in a risk to the rights and freedoms of data subjects. If such a risk is unlikely then the breach will not be reported to the ICO, but will be recorded in the data breach template. Remedial action will be identified, and a timetable for completion will be drawn up.

If there is a risk to data subjects, the Chair will notify the ICO of the breach, describing:

a) the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
b) the name and contact details of the person from whom more information can be obtained. This may be the Chair, or it may be some other person assigned responsibility for handling the data breach
c) the likely consequences of the personal data breach
d) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

This notification will take place within 72 hours of the Chair being notified of the breach, unless this is not possible, in which case it will take place as soon as possible, and reasons given for the delay.

Where it is not possible to provide all of the above information at the same time, the information may be provided in phases without undue further delay.

The Chair will record the breach in the template, stating the nature of the breach, when and how it was reported, when it was notified to the ICO, its effects and the remedial action taken, and any response from the ICO, including any mandated action.

Notification to data subject(s)

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, and it is not possible to prevent this risk from materialising, the Chair will inform the data subject(s) without undue delay. The following information will be communicated, using clear and plain language:

a) The nature of the personal data breach
b) the name and contact details of the person from whom more information can be obtained. This may be the Chair, or it may be some other person assigned responsibility for handling the data breach
c) the likely consequences of the personal data breach
d) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

The notice must be sent directly to the data subject, unless this would involve disproportionate effort, in which case it can be published on the website.

Delegation

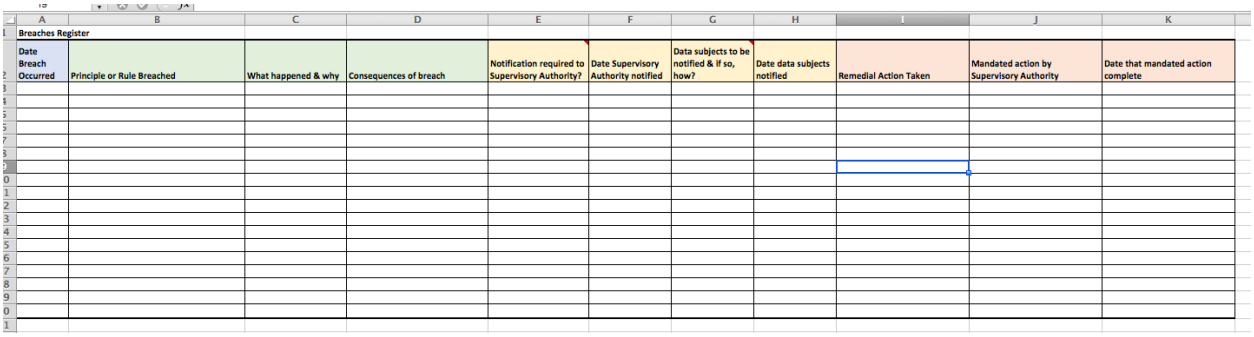
The Chair may delegate their responsibilities under this section to a named person, but will continue to hold ultimate responsibility for ensuring that any breach is properly recorded and (if relevant) notified.

Version

This policy was drafted on 5th May 2020, and approved by the R9 Board on [INSERT DATE]. Any questions about this policy or any queries concerning data protection matters should be raised with the R9 Chair (chair@oaregion9.org)

4. Data Breach Log

Excel document –sample (actual log resides in the R9 GDPR dropbox)

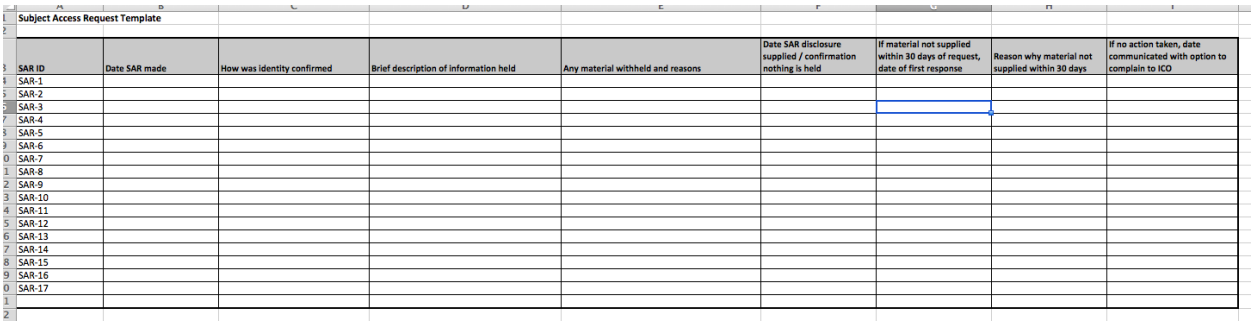


Breaches Register

Date Breach Occurred	Principle or Rule Breached	What happened & why	Consequences of breach	Notification required to Supervisory Authority?	Date Supervisory Authority notified	Data subjects to be notified & if so, how?	Date data subjects notified	Remedial Action Taken	Mandated action by Supervisory Authority	Date that mandated action complete

4a. Subject Accesss Request Log

Excel document –sample (actual log resides in the R9 GDPR dropbox)



Subject Access Request Template

SAR ID	Date SAR made	How was identity confirmed	Brief description of information held	Any material withheld and reasons	Date SAR disclosure supplied / confirmation nothing is held	If material not supplied within 30 days of request, date of first response	Reason why material not supplied within 30 days	If no action taken, date communicated with option to complain to ICO
SAR-1								
SAR-2								
SAR-3								
SAR-4								
SAR-5								
SAR-6								
SAR-7								
SAR-8								
SAR-9								
SAR-10								
SAR-11								
SAR-12								
SAR-13								
SAR-14								
SAR-15								
SAR-16								
SAR-17								

5. Assembly Form Privacy Notice

Important notice to all R9 Assembly Attendees

This privacy notice provides information on how Region 9 of Overeaters Anonymous collects and processes the personal data which you supply when you register for the R9 Assembly and / or Convention. We process your data in accordance with the General Data Protection Regulation (EU) 2016/679.

1. IMPORTANT INFORMATION AND WHO WE ARE

Overeaters Anonymous is a worldwide fellowship, with different bodies making up the service structure to support local groups. The service structure is fully described here: https://oa.org/groupsservice-bodies/groups/service-structure/

Region 9 is composed of groups, intergroups, and service boards across Europe, the Middle East, Africa, and Western Asia. Region 9 is the controller and responsible for your personal data. Our full name is 'Overeaters Anonymous Region 9'.

The Region is served by the Region 9 Service Board, and the OA Trustee for Region 9. In this notice, 'Board' should be taken to include the Trustee for Region 9. There are also three standing committees which support the Board: Translations, Public Information and the General Committee. From time to time there may be set up 'ad hoc' or temporary committees to undertake specific pieces of work. The committees are made up of one Board member, together with Regional Representatives to the Assembly, and individual OA members who offer service.

If you have any questions about this privacy notice or our data protection practices, please contact us at privacy@oaregion9.org.

2. THE DATA WE COLLECT ABOUT YOU

a) Attending the Assembly / Convention in a personal capacity

We collect your name and contact details for the purposes of distributing the Assembly / Convention business papers and communicating with you about the Assembly / Convention (both beforehand and after it has finished).

Our legal basis for processing this information is our legitimate interest in carrying out the routine administration and business of the Assembly / Convention. We keep this information for four months after the last day of the Convention.

b) Region 9 Representative to the Assembly

Being a Region 9 Representative is a service position that Intergroups elect for varying time periods. During this time you are the contact point for your Intergroup for Region 9. Your details will be kept securely on file for this purpose, and you may be contacted by the Region 9 Service Board or R9 Committees during this time.

We also use your personal information to establish quoracy at the Assembly.

Our legal basis for processing your information is our legitimate interest in carrying out the business of the Region with elected representatives. We keep your details on file for 2 years 3 months after this assembly.

If you resign your service position and wish for your details to be deleted then please contact us at privacy@oaregion9.org.

c) Data you can choose to share

In our experience, people who attend Assembly / Convention often wish to offer wider service to the fellowship. This might be through volunteering to support a committee, or undertaking some of the work of Region 9. If you do volunteer or offer service to Region 9 in any other way then we will need to keep your contact information so that we can keep in touch with you. The legal basis on which we process this information is your consent, which you will be asked for at the time you sign up for service. Your contact information will be kept securely for five years from the closing date of the assembly and will then be deleted, unless you give further consent for us to keep it. You can also ask for your contact details to be deleted at any time.

One of the ways that you could offer service is to be a contact person within your country for OA Region 9. This would mean that members of the Region 9 Service Board or Committees would have access to the contact details that you supply, and could approach you if someone needs to get in touch with an OA member in your country / area. This might be a newcomer, or a professional. We would not pass your details on without contacting you and asking if you consent for this to happen. **If you are happy to go onto this outreach list then you should tick the question below**. We would then keep your details on the list until you tell us to remove them. You can ask for your details to be deleted at any time.

You can also choose to sign up to the Region 9 weekly announcements email list, which means that we will need to process your name and email address. **You can do this by ticking the question below.** The legal basis on which we process this information is your consent. We will

keep your details on this list unless you unsubscribe. You can unsubscribe from the list at any time by clicking the Unsubscribe link at the bottom of each email.

3. HOW WE USE YOUR PERSONAL DATA

We will only use your personal data for the purposes for which we collected it as described above. Only authorised people are permitted to access your data, which is kept secure and confidential for the time period as described above, and then deleted / destroyed using secure methods.

4. HOW WE SHARE YOUR PERSONAL DATA

We do not share your data with anyone outside Region 9 OA unless you have specifically consented to this, or we are required to share the information by law.

We make use of IT tools (e.g. email, cloud hosted storage) which mean that your data is processed by third parties (e.g. Google), but we always have in place GDPR-compliant data processing agreements to protect the privacy of your data.

5. INTERNATIONAL TRANSFERS

Region 9 encompasses countries outside the European Economic Area, and so your data may be transferred outside the EEA. We need to tell you this because countries outside of the European Economic Area (EEA) do not always offer the same levels of protection to personal data, so European law has prohibited transfers of personal data outside of the EEA unless the transfer meets certain criteria.

We will only transfer your data outside the EEA on the following, lawful, grounds:

a) The country has been approved by the EU as having an adequate standard of data protection

b) You are a resident of a non-EEA country, and so we must process your information outside the EEA in order to communicate with you

c) We are using a third-party data processor which stores or processes information outside the EEA (e.g. Google processes information in the US). We will only use such a processor if there are EU-approved safeguards for the security of data, e.g. the processor has signed up to the EU-US Privacy Shield, or our processing contract incorporates EU-approved Standard Contractual Clauses.

d) You have explicitly consented to the transfer of your information, and you have been

warned of the possible risks of the transfer

Important note about transfers outside the EEA under (d) above (consent):

The Region 9 Service Board may include OA members who come from areas outside the EEA, due to the wide geographical scope of the Region. In carrying out the business of the Region the Board will need to communicate via email, and we also use a shared Dropbox folder. If a Board member receives an email containing personal data outside the EEA, or makes use of the Dropbox folder to access personal data from outside the EEA, **they will be transferring that data outside the EEA**.

Depending on the country where the Board member is based, the EU may have made a finding that there are adequate data protection standards in place. However, it is possible that the Board member is based on a country where there is no such finding.

We only share information between Board members where this is genuinely and reasonably needed to conduct the business of the Region. For example: the Secretary will access the list of email addresses in order to send out minutes, and the General Officer will use the list of people who have sign up to receive announcements in order to send them out. All Board members are bound by data protection policies, and information security policies, and will be required to delete information as directed.

In order for us to carry out the business of the Region lawfully, we need to address the possibility that your personal data is accessed by a Board member who is based outside the EEA in a country where the EU has not made a finding of adequacy. **We therefore need your consent** for your personal data to be accessed from outside the EEA. At the bottom of this form you will be asked to give your consent.

6. YOUR LEGAL RIGHTS

Under certain circumstances, you have rights under data protection laws in relation to your personal data:

a) the right to receive a copy of the personal data we hold about you;

b) the right to request rectification or erasure of your personal data, or restriction of processing concerning you, or to object to processing;

c) where processing is based on consent, the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

d) the right to lodge a complaint with a supervisory authority for data protection In the UK this is the Information Commissioners Office (www.ico.org.uk).

If you would like to exercise any of these rights then please contact us at chair@oaregion9.org.

Please sign this form on the next page.

Please sign below to show that you have read and understood this privacy notice. Please contact us if you have any questions.

☐ ***VERY IMPORTANT:*** ***I consent for my data to be transferred outside the EEA between Region 9 committee members as described at paragraph 5 above.***

☐ ***Outreach:*** ***Please tick here if you would like to go onto the 'outreach' list. Your details may be shared with the Region 9 Board and Committees, but you would be contacted to ask if you consent for them to be given to anyone else.***

☐ ***Announcements:*** ***Please tick here if you would like to be added to the Region 9 weekly announcements email list.***

Signed: ..... Date: .....

Name: .....