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)