

DATA PROCESSOR AGREEMENT

BETWEEN

Overeaters Anonymous Region 9

AND

Overeaters Anonymous [*insert name of territory / country*]

THIS AGREEMENT dated [*date*] is BETWEEN:

- (1) The 'Controller': Overeaters Anonymous Region 9, a not-for profit organisation registered in England and Wales with HM Revenue and Customs number 682 54283 05163 A
- (2) The 'Processor': Overeaters Anonymous [*insert name of territory / country*]

WHEREAS:

- (a) The Controller is a Region of Overeaters Anonymous and is required by Article VII of Subpart B of the Bylaws of Overeaters Anonymous, Inc. to hold a Regional Assembly for the election of officers and the selection of nominees for regional trustee.
- (b) The Controller will also hold a Convention for OA members, to take place in the same venue immediately after the Assembly.
- (c) The Processor has agreed to host the [*year*] Regional Assembly and Convention in [*location*], between [*dates*].
- (d) The hosting of the Assembly will require the Processor to undertake the processing of personal data on behalf of the Controller.

IT IS HEREBY AGREED AS FOLLOWS:

Definitions

1. The Processor will process personal data in accordance with the General Data Protection Regulation (GDPR) (EU) 2016/679 [and *insert name of any local data protection legislation which also applies*] ('the Data Protection Laws'). The meaning of "*italicised*" terms in this agreement are as defined in the GDPR.
2. The *personal data* will include:
 - a. Names and contact details for people attending the Assembly;
 - b. Names and contact details for people attending the Convention;
 - c. Names and contact details for members of Region 9 Service Board and Committees;

- d. Names and contact details for people who make contact with the Processor about the Convention.
3. The two sides agree that for the purposes of processing this personal information the Controller is a *Controller* and the Processor is a *Processor*.

Data Protection

4. The Processor shall comply with the Data Protection Laws in connection with the processing of this personal data. The Processor shall also ensure its sub-processors and each of their personnel shall comply with the Data Protection Laws in connection with the processing of this personal data.
5. In processing this personal data on behalf of the Controller, the Processor will comply with Article 28 of the GDPR. This means that they will:
 - a. Take instructions from the Controller as to what they will do with the personal data, and follow those instructions.
 - b. Make sure that anyone working with or for the Processor will treat the personal data in confidence.
 - c. Use appropriate security measures to protect the data from destruction, loss, alteration and unauthorised disclosure.
 - d. Get permission from the Controller before sharing the data with anyone else, including any other processor.
 - e. Work with the Controller to make sure that data subjects can access their data, or apply for it to be removed or updated, or for processing to be restricted in any way.
 - f. Help the Controller to comply with the legal duty to report data breaches.
 - g. Return all the personal data to the Controller after the Assembly / Convention has finished, and keep no copies of it.
 - h. Cooperate with the Controller if asked to take part in any data security checks or audits.

Data Subject Requests

6. An individual whose data is processed by the Controller or Processor is called a 'data subject'. Participants in the Assembly and Convention are data subjects.
7. The Processor shall pass on to the Controller all communications received relating to personal data as soon as possible (and in any event within three days of receipt).
8. The Processor and Controller will cooperate to respond to such requests and communications in compliance with the requirements of the GDPR.

Processing outside the European Economic Area (the EEA)

9. The Processor will not process and / or transfer any personal data to countries outside the EEA without the prior written consent of the Controller. The Controller grants the Processor permission to use the following named third party providers based outside the EEA and which have agreed to be bound by the EU-US Privacy Shield to process personal data under this Agreement:
 - a. Dropbox (cloud hosting of documents) certificate [here](#)
 - b. *[insert any other third party providers]*

Personal data breach

10. The Processor shall promptly (and in any event within 24 hours) notify the Controller if it suspects or becomes aware of:
 - a. Any accidental, unauthorised or unlawful processing of the personal data; or
 - b. Any suspected, actual or threatened occurrence of any personal data breach in respect of any personal data.
11. Where the Processor becomes aware of (a) and / or (b) at paragraph 9 above, it shall, without undue delay, also provide the Controller with the following information:
 - a. Description of the nature of (a) and / or (b), including the categories and approximate number of data subjects and personal data records concerned;
 - b. The likely consequences; and
 - c. Description of the measures taken, or proposed to be taken to address (a) and / or (b), including measures to minimise possible adverse effects.
12. The Processor and Controller shall cooperate to investigate the matter, and to ensure that any breach be notified to the Supervisory Authority and affected data subjects in accordance with the GDPR.
13. The Processor will not inform any third party of any Personal Data Breach without first obtaining the Controllers' prior written consent, except when required to do so by law.

Term and termination

14. This Agreement will remain in full force and effect so long as the Processor retains any Personal Data related to the hosting of the Assembly and / or Convention.

Signed

For and on behalf of **OVEREATERS ANONYMOUS REGION 9**

Signed: Date:

Name (block capitals):

Position:

For and on behalf of **OVEREATERS ANONYMOUS [*insert territory or country*]**

Signed: Date:

Name (block capitals):

Position: