

The BABAO Data Protection Policy

This document outlines the measures that the BABAO committee will take to comply with GDPR regulations.

Approach to data protection

Personal data will be held by the Membership Secretary alone. Trustees may ask for personal data to correspond with specific groups within the membership, or for financial purposes. Data will be transferred between Trustees using password protected files, and the files will be securely deleted after use. The Membership Secretary is responsible for making sure that the personal data are held on an encrypted and password protected device, and that data are securely passed between the Membership Secretary and other Trustees. Data will not be used for any other reason, other than that specified at the time of request from the Membership Secretary, and will not be stored by any Trustee. There is no need to complete a Data Protection Impact Assessment because our data processing is unlikely to result in a high risk to individuals.

Compliance with Data Protection Policy

There will be an annual review of the policies to monitor compliance by the Data Protection Lead and results will be reported to Trustees. The Data Protection Lead will also report quarterly to the Trustee meetings to maintain awareness and vigilance about GDPR compliance, and to update Trustees about any breaches or concerns that are raised by our members.

Process for dealing with data information requests

Members can view the information that is currently held about them. To request this members contact the BABAO Membership Secretary (currently Anwen Caffell at membership@babao.org.uk), copying in the Data Protection Lead (currently Catriona McKenzie at c.mckenzie@exeter.ac.uk).

Members wishing to amend or update any information, can complete the 'Updating Your Details' form which is available on the BABAO website: <http://www.babao.org.uk/membership/#updatingdetails>.

Completed forms should be sent to membership@babao.org.uk. We will correct any out of date information within one month and confirm that the information has been updated.

Members wishing to delete, restrict or object to the processing of their personal data, are encouraged to contact the Membership Secretary and the Data Protection Lead on the email addresses provided above. It is necessary for us to hold certain information about

members in order to run the organisation, but we will be happy to discuss any concerns, and remove unnecessarily stored information. The outcome of the request will be documented.

If Trustees receive a verbal request about personal data, they will forward the information to the Membership Secretary and the Data Protection Lead. All requests for updating personal data will be dealt with within one month.

Process for dealing with a security breach

If there is a security breach this should be reported immediately to the Data Protection Lead. They will put mechanisms in place to investigate and implement recovery plans if possible. Affected individuals will be contacted to inform them about the breach, and if necessary the event will be reported to the ICO (Information Commissioner's Office), the independent regulator which exists to protect people's information rights. All data breaches will be documented by the Data Protection Lead, even if they do not need to be reported to the ICO.

Making a complaint

Members who are unhappy about the way we are managing and using personal information, should email the Data Protection Lead, (currently Catriona McKenzie at c.mckenzie@exeter.ac.uk).

If we are approached by any member who is unhappy about us holding specific information, the request will be considered in the first instance by the Membership Secretary and the Data Protection Officer and the outcome of the request will be documented.

If after correspondence a member is still unhappy, they have the right to complain to the ICO.