BABAO Personal Data Breach Policy 2021

The following documents the steps that will be taken in the case of a personal data breach within the British Association for Biological Anthropology and Osteoarchaeology (BABAO).

Allocation of Responsibility

In the case of a personal data breach within BABAO, the Data Protection Lead (DPL) will take the role of Data Protection Officer (DPO) and will work in consultation with the Data Controller (the current Membership Secretary, MS) and with BABAO's President to manage the situation.

Current DPL: Rebecca Avery (rebecca.avery97@hotmail.co.uk)

Current MS: Bennjamin Penny-Mason (academia@bennjaminpm.com)

Current President: Rebecca Redfern (rredfern@museumoflondon.org.uk)

Information Commissioner's Office (ICO)

Definition of Personal Data Breach

The ICO's definition of a personal data breach is:

"*a security incident that has affected the confidentiality, integrity or availability of personal data*. *In short, there is will be a personal data breach whenever any personal data is accidentally 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.*"

Breaches can be accidental or deliberate in their cause and can include: accessed by an unauthorised third party; deliberate or accidental action by a controller or processor; sending personal data to an incorrect recipient; computing devices containing personal data being lost or stolen; alteration of personal data without permission; and loss of availably of personal data.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#whatisa

Response Plan

When the personal data breach is reported the Trustee to whom it is reported or who reports it themselves will immediately contact the DPL and give them all the information they have regarding the incident.

The DPL will then contact the MS and the President. The DPL and MS will work to trace the source of the breach and will assess the severity and act accordingly. The President, as the face of BABAO, will communicate with the membership as necessary. If the breach is deemed severe enough the ICO will be contacted within 72 hours where feasible.

The membership should be contacted without undue delay if the breach is likely to result in a high risk of adversely affecting their rights and freedoms. This letter will be based of the draft found at the end of this document and will be written by the DPL and the President.

The DPL will instigate an investigation into the incident and will submit a report to the Board of Trustees within 2 weeks of the incident taking place. The situation will also be discussed at the next Board meeting.

The Personal Data Breach Register will be updated regardless of the severity of the breach and any outcomes.

Assessment of Risk

When a breach is reported it will be assessed to establish the potential risk to individuals. The DPL will take into account the nature of the incident, the severity of potential impact and the level to which it could have been avoided.

Reporting to the ICO

A breach will be reported to the ICO if it is likely that there will be adverse effects on the rights and freedoms of individuals. A non-report needs to be justified and recorded in the breach log.

Processors

Any processors that BABAO uses must inform the DPL of a data breach with undue delay.

Contacting Individuals

Members will be contacted with undue delay, as a priority, if the breach will adversely affect them. An email similar to the one found at the end of this document will be sent by the president to those affected.

Continuing Response

Following a personal data breach, a data protection review will be carried out and presented to the Board. The Board may elect to refresh their GDPR training; may suggest necessary changes that need to be made to avoid similar incidences; or may consider asking for external help.

The Board will be prepared to receive an increase in data requests from the membership following a breach.

Example of communication to membership following personal data breach - this is a very basic draft and will be edited to make it more specific in the event of a breach.

Dear Member,

I am contacting you to inform you of a recent security incident which involved technology which potentially held some information about you.

Whilst we are unaware of any actual misuse of your information, out of an abundance of caution we wanted to give you some information about the event so that you can understand what happed, how you may be involved, the steps we have taken and some steps you can take in response.

We would like to reassure you that this incident is now resolved, and that full payment card information was not compromised.

What Happened?

***details of the incident**

What we have done

details of BABAO's response

As an organisation, the security of data, including your information is a top priority and we take the protection of personal and business data very seriously.

We have taken various additional steps to further strengthen the security of our systems. Please rest assured that our systems are secure, our website remains fully operation and that BABAO is a safe organisation to be a part of.

What information was involved?

details of information involved

steps for members to take in response

We would like to take this opportunity to remind you of your rights as an individual regarding your data which can be found in our data protection policy. https://babao.org.uk/data-protection/

Yours sincerely,

Rebecca Redfern, President