Data Protection Policy and Information

October 2018

The Policy

New data protection regulations (General Data Protection Regulations) that come into effect on 25 May 2018 in the UK require that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

It is The AOI's responsibility to comply with and demonstrate compliance with these principles.

Full details can be found at the ICO at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Definitions

Personal Data: Data which relates to a living individual who can be identified for those data or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller. This includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

Data Controller: The person or organisation who determines the purposes for which and the manner in which any personal data are, or are to be processed. In this instance the AOI is the data controller.

Data processor: a natural or legal person, public authority, agency of any other body which processes personal data on behalf of the controller. Details of the AOI's processors can be found in section 4.

Data Subject: The identified or identifiable living individual to whom personal data relates. The Data Protection Act 1998 (still in force until it is repealed by the Data Protection Act 2018) and the GDPR do not apply to individuals who have died or who cannot be identified or distinguished from others.

1. AOI, Data Protection and Governance

1.1 The board will be briefed about the policy on commencement & will review the policy annually as part of the overall risk assessment of the AOI.

1.2. The AOI staff will be briefed in advance of the policy commencement about their responsibilities in relation to data protection. This will be reviewed annually to ensure that the AOI's policy reflects our practices and complies with the law.

2. AOI Data

2.1 The AOI holds various categories of personal data. Data Subjects may appear in more than one category:

Data Subject	How it is used	Where the data comes from	What data is held	How the data is held and processed	Who AOI share the data with	Our Lawful basis for processing	Length of time data is kept & rationale for use
Active members	Providing membership service Debt recovery	Individuals themselves	Names, emails, post address, agent (if given), college (if given), folio images (if given), financial transaction history, record of past membership with AOI, record of helpline enquires to AOI, bank details	Secure server Paperwork in locked office and secure archive With data processors, e.g. payment processors	No other organisation*	Contract	Duration of contract (it is not possible to service the contract without data retention) Contact, Finance & helpline details kept for 7 years (legal requirements, e.g. for tax purposes)
Resigned & lapsed members	Records kept for archive; Industry updates	Individuals themselves	Names, emails, post address, financial transaction history, record of past membership with AOI, record of helpline enquires to AOI, bank details	Secure server Paperwork in locked office and secure archive With data processors, e.g. payment processors	No other organisation	Legitimate interest	Contact details kept in perpetuity (members often renew membership after many years. Occasionally an illustrator is found through the AOI, providing them with royalties / commissions) Contact, finance & enquiries details kept for 7 years (legal requirements, e.g. for tax purposes)

							Industry updates: 1 year (resigned & lapsed members will receive monthly industry updates for 2 years after resignation the AOI has provided services (membership) in the past and there is commercial interest to continue providing this service)
Business contacts	Day to day running of AOI	Collated from public sources or given by individuals	Names, emails, postal and phone, record of interaction with the AOI, bank details where financial transaction are made	Secure server Paperwork In locked office and secure archive With Data processors, e.g. payment processors	No other organisation	Consent	5 years from interaction (AOI engages past contacts over long cycle programmes) Contact and Finance kept for 7 years
Directories	Commissioners details included in AOI Directories, and sold through AOI	Collated from public sources and ratified by individual	Names, emails, postal, phone, job title and relevant job history	Secure server Data processors as detailed below	Customers	Specific Consent to sharing data with third party	5 years from interaction (Note that data subjects are contacted annually for inclusion and must explicitly opt in.)
Award entrants - active & historical	Processing awards Marketing of awards	Individuals themselves	Names, emails, post address, financial transaction history, entered images, accompanying entrance info, record of award outcome.	Secure server Paperwork in locked office and secure archive Data processors as detailed below	Award partners (as per t&c's)	Specific Consent (included in terms – going forward tickbox before	3 years from award entry (Assume it is in the interests of previous entrants as related to what ordered before and is in mutual commercial interest.)

				Publically available catalogue (shortlist)		participants enter awards) Legitimate interest	
Current and past staff, patron and board	Sharing info about AOI HR & Finance needs	Individuals themselves	Names, emails, postal address, phone, next of kin, photographs, payroll and HR interview & performance records	Secure server Paperwork in locked office and secure archive Data processors as detailed below	No other organisation	Consent	Contact details kept in perpetuity (Occasionally an illustrator is found through the AOI, providing them with royalties / commissions. The AOI aims to preserve the heritage of illustration and will engage in historical reviews) Finance and HR records kept for 7 years (legal requirements)
Potential members	Targeted marketing & industry news	Collated from public sources e.g. trade fairs / individuals themselves	Names, emails	Server Data processors as detailed below	No other organisation	Legitimate interest (Data subjects pro actively shared their contact details with the industry. AOI believes they are interested in our services because of the	12 months

						professional context)	
Shop customers (who are not members)	To process order/contract Debt recovery		Names, postal, email, phone, financial history and bank details, mailing house (for subscribers)	Secure server Paperwork in locked office and secure archive Data processors Finance in secure archive	No other organisation	Consent	12 months Contact, finance and HR records kept for 7 years (legal requirements)

2.2 The AOI considers their bases for controlling and processing data lawful as data subjects have either:

2.2.1. entered into a contract with the AOI to provide specific goods or services;

2.2.2. given their consent in order to provide membership services;

2.2.3. the AOI can show legitimate interest as data subjects have purchased services before or entered into negotiations as to purchasing services from the AOI; or

2.2.4. data subjects have offered their details and the AOI has collected their personal data in a professional context (e.g. trade fair) and has reason to believe that they are interested in the AOI's services and information.

The AOI has checked that processing is necessary for its purpose and there is no other reasonable way to achieve the purpose.

2.3 Where consent is required, this will be

2.3.1. done in a transparent manner through the form of a tick box separate to any other terms and conditions or agreements.

2.3.2. Specific and 'granular'. It will name third party controllers and signpost how people can withdraw consent easily without detriment.

2.4 The AOI will keep a record of those who have explicitly given consent, when they gave consent and the purpose for which they have given consent (e.g. marketing preferences).

2.5 The AOI will review the bases by which it processes data at least annually, and in any case when there is a specific change in supplier or business.

2.6 The AOI will act swiftly if anyone withdraws consent and will not penalise that individual. The membership team is responsible for processing such enquiries.

2.7 The AOI will communicate with data subjects whose details are contained in the existing database (as per section 2 above). It will continue to use existing data for the purposes listed above and based on lawful reasons, unless an individual specifically withdraws consent or informs us that it wishes us to stop processing data for a particular purpose.

2.8 In 2018 (and historically) the AOI has shared data with US based Directory of Illustration in order to honour a contract to provide reciprocal portfolios. The AOI will explicitly state that in its Privacy Policy that this means data is shared outside of the EEA.

3. AOI Data processors

3.1 The AOI holds data electronically as well as physically. Where data is held electronically details are given in the next section. Physical records are kept at Somerset House which has effective security. AOI offices are locked when empty, and sensitive data is kept in a locked file.

3.2 All data is held within the UK, apart from data shared with Mailchimp which is USA based, but has a data shield policy in place.

Organisation	Types of Data Processed	Compliance

Digital Ocean	Cloud back up of internal computer system including personal data	https://www.digitalocean.com/legal/privacy-policy/
Names Co	Email provider with cloud based storage of emails	https://www.names.co.uk/info/terms/privacy-policy
Mailchimp	Names and email addresses	https://mailchimp.com/legal/privacy/
Sage	Names, addresses, bank details and financial transactions	https://www.sage.co.uk/uk/hrpayrollhero/privacy-policy
Woo commerce	Finance details	https://www.gdprwp.com/privacy-policy/
Go Cardless	Financial details	https://support.gocardless.com/hc/en-gb/articles/360000281005
Aviva Pensions	HR information used to process pensions	https://www.aviva.co.uk/legal/privacy-policy.html
Mailing Houses	Names and mailing addresses to send Varoom	Supplies change and will be checked
HSBC	Bank details in order to make payments	https://www.hsbc.co.uk/content/dam/hsbc/gb/pdf/privacy-notice.pdf

4. What to do if the data AOI holds is inaccurate?

4.1 As demonstrated, the AOI only shares certain data. If it were found to be inaccurate the following actions will be taken to remedy it:

Data	Action if inaccurate
Directories	Amend directors and circulate update to all customers
Award entries	Amend records and circulate to partners
All other data	Amend records

5. Privacy Notice

5.1 The AOI privacy notice explains, in plain English:

a. Our identity and how we intend to use individual's personal data;

b. Our lawful basis for processing data;

c. Our data retention periods see point e) on page 1 - for no longer than is necessary for the purposes for which the personal data are processed;

d. The individual's right to complain to the ICO if they think there is a problem in how we handle their data.

5.2 The AOI will review the privacy notice available online annually.

6. Meeting Individuals' Rights

6.1 The AOI meets the following rights for individuals:

Relevant right	How the AOI meets it
Right to be informed	Privacy policy on the website clearly stating how we use data
Right of access	All data will be made available in a readable format on request by the individual
Right to rectification	All data can be swiftly amended on request by the Membership Manager
Right to erase	Membership Manager to remove from Filemaker database, social media and wordpress database. Only a basic record (name) will be kept to avoid that individual's data will be entered again and processed.
Right to restrict processing	AOI will cease using data on request to do so and inform partners if appropriate. Only a basic record (name) will be kept to avoid that individual's data will be entered again and processed.
Right to data portability	Membership Manager to export as a csv file on request
Right to object	Everyone has the right to challenge where appropriate.
Rights re automated decision making and profiling.	Not applicable to AOI

7. Handling Data requests

7.1 The AOI will respond to all data requests within 30 days as required by law. It will not charge for any reasonable requests. If the request is excessive or unfounded The AOI may choose to refuse or charge for the request.

7.2 If the AOI refuses a request the individual will be told why and that they have the right to complain to the ICO and seek a judicial remedy. This will be communicated as soon as possible or within 30 days from receiving the individual's request.

8. Security and Data Breaches

9.1 A data breach is broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a breach when any personal data is lost, destroyed, corrupted, or disclosed; if it is accessed without authorisation or if it is made unavailable and this unavailability has a significant impact on individuals. It can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor

- Sending personal data to an incorrect recipient
- Devises containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of persona data

9.2 The AOI work with it's retained IT provider and have identified the following means to ensure the safety of data, and if required detect data breaches:

Action	Outcome	Process
Computers and devices		
Antivirus installed on all computers	Preventative	Review annually with IT provider
Activate Firevault on macs	Preventative	Activate once
Install System Manager on all computers	Breach Detection	Review annually with IT provider
No personal data stored on laptop / ipad	Preventative	Brief staff and review annually
No personal data to be stored on USB sticks or portable devices	Preventative	Brief staff and review annually
Office to be locked nightly and when unattended	Preventative	Brief staff and review annually
Server		
Restrict remote access to server	Preventative	Activate once
Increase block out policies on server	Preventative	Activate once
Emails		
90 day password change on staff emails	Preventative	Brief staff and review annually

9.3 Where a data breach occurs it will be fully investigated to understand how a recurrence can be prevented, either through better processes, training or corrective steps.

10. Responding to a Data Breach

10.1 The AOI will recognise a data breach by either

10.1.1 physical or electronic evidence such as a visible hacking or break in

10.1.2 alerted by software

10.1.3 alerted by third party including customers, service providers

10.2 All breaches will be documented, regardless if they need to be reported or not. If they are not reported the rationale for that decision will be documented.

10.3 The AOI are controllers and we work with several processors including Mailchimp, woo commerce and Global Iris. If a processor informs us of a breach, we will inform the ICO.

10.4 Where a data breach occurs, and it is deemed likely to result in risk to people's rights and freedoms, the AOI will inform the ICO **within 72 hours of becoming aware of the breach**

(even if the full details are not known) where feasible.

10.5 If the breach is likely to result in a high risk of adversely affecting individuals rights and freedoms, those individuals will be informed without undue delay by email.

10.6 The AOI will assess the potential impact of a data breach to individuals rights and freedoms by considering the potential adverse impacts using a matrix as below:

Potential Adverse effect	Description	Risk level: Low, medium, high
Physical or material damage		
Loss of control over data		
Limitation of rights		
Discrimination		
Identity theft / fraud		
Financial loss		
Reputational damage		
Inconvenience		

10.7 Should a breach occur The AOI will provide the ICO with the following information

10.7.1 A description of the nature of the breach including (where possible) the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned.

10.7.2 Contact details of a person at the AOI from whom more information can be obtained.

10.7.3 A description of the likely consequences of the personal data breach.

10.7.4 A description of the measures taken, or proposed to be taken to deal with the breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

10.8 Should a breach occur The AOI will provide affected individuals with the following information in clear, plain language:

- Contact details of a staff member at the AOI who can be contacted for further information.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken to deal with the breach including, where appropriate, measures taken to mitigate any possible adverse effects.
- How to protect themselves from its effects

11. Privacy Impact Assessment

11.1 Having considered the risk, the AOI has decided that it does not need a PIA.

12. International

12.1 The AOI has members worldwide, however it operates solely from the UK, and therefore the ICO is the supervisory authority.

13. Children

13.1 The AOI does not hold information, or intend to hold children's data. Should this change the policy will be reviewed.

14. Images

14.1 Where an image of a data subject is used, this will be with permission secured via email. Where an image is made at an event, permission will be sought on a case by case basis.