AIA
THE ASSOCIATION OF INTERNATIONAL ACCOUNTANTS

General Data Protection Regulation (GDPR) Policy

General Data Protection Regulation (GDPR)

1.0 Introduction

The Association of International Accountants (AIA) is required to collect information about individuals to carry out its functions as a recognised professional accountancy and membership body and to act in accordance with relevant legislation and regulatory requirements.

Within this policy personal data is defined as 'information which relates to a living individual and from which they can be identified, either directly or indirectly'. This data may also include private and confidential information as well as sensitive information, whether in paper, electronic or other form.

Irrespective of how information is collected, recorded and processed person-identifiable information must be dealt with properly to ensure compliance with the General Data Protection Regulation (GDPR) and any relevant regulatory requirements or legislation.

In undertaking its business AIA creates, gathers, stores and processes data on a variety of subjects such as on members and students (both potential, current and former), employees and contractors, suppliers and general contacts. The use of personal data for Members and Students ranges from personal information, financial transactions, qualifications, employment, training and disciplinary action throughout the lifetime of their membership.

On occasion, some of the data collected and processed will be sensitive data, i.e. data concerning a subject's racial or ethnic origin, physical or mental health.

The GDPR places obligations on the AIA and the way it handles personal data to ensure personal data is processed fairly, lawfully and securely. This means that personal data should only be processed if there is a valid condition of processing (e.g. consent obtained from the data subject, or forms part of the legitimate interest of the organisation). There are restrictions on what can be done with personal data such as passing personal information on to third parties, transferring information outside the EU or using it for direct marketing.

2.0 Purpose of Policy

This policy sets out the responsibilities of the AIA to comply fully with the provisions of the GDPR.

The policy applies to all staff and relates to any item of personal data that are created, collected, stored and/or processed through any activity of the AIA including overseas branches and partners, across all areas of membership, examinations, marketing, finance and professional services.

Related policies include the AIA Information Security Policy, ICT Procedures, Risk Management and Disaster Recovery Procedures and the AIA Privacy Policy.

3.0 Data Protection Principles

AIA is required to adhere to the six principles of data protection as laid down in the GDPR, which means that information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The six principles are:

1. Personal data shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes. Further processing for archiving, historical research or statistical purposes is permissible ('purpose limitation').

3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed ('data minimisation').
4. Personal data shall be accurate and where necessary kept up to date ('accuracy').
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose ('storage limitation').
6. Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

4.0 Personal Data

Personal data is information about a living individual, who is identifiable from that information or who could be identified from that information when combined with other data which the AIA either holds or is likely to obtain. GDPR also refers separately to 'special categories' of personal data which includes particularly sensitive personal information such as health details, racial or ethnic origin or religious beliefs. Further information and guidance on personal data, including how AIA categorises individuals and the justification for holding and using that data is detailed in Appendix 1.

The definition of 'processing data' includes obtaining/collecting, recording, holding, storing, organising, adapting, aligning, copying, transferring, combining, erasing and destroying the information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure.

AIA remains responsible for the control of personal data it collects even if that data is later passed onto another organisation or is stored on systems or devices owned by other organisations or individuals.

We do not knowingly collect, use or share information that could reasonably be used to identify children under the age of 16 without prior parental consent or consistent with applicable law.

5.0 Data Breaches

AIA employees, past and present, have a contractual obligation to protect AIA's information assets, systems and infrastructure. They are required at all times, to act in a responsible, professional and security-aware way and to fully comply with the GDPR and related policies.

Examples of personal data breaches include:

- Loss or theft of data or equipment
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

Employees are required to:

- Identify any security shortfall in existing practice.

- Immediately report any software malfunctions, security incidents, suspected viruses, faults, weaknesses or threats, observed or suspected, to the AIA Data Protection Officer.

All actual or suspected security incidents are reported to the AIA Data Protection Officer who will undertake the following measures:

- Identify breach - identify how the breach has occurred, for example, whether this is an online attack or data leakage caused accident or intention.
- Investigation and containment - whether internal or external, identify how to restore security considering the breach.
- Impact assessment - once the breach is resolved, a risk assessment will be conducted for individuals and AIA.
- Recovery - repair the data and systems so that AIA can continue to operate.
- Notification and communication - establish a communication strategy to inform those individuals affected that a data breach has occurred and report the incident to the Information Commissioner's Office no later than 72 hours after the breach is discovered.
- Evaluation and improvement – all incidents will be fully investigated and evaluated and if necessary changes made to increase security measures.

6.0 Conditions of Processing and Consent

For it to be legal and appropriate for the AIA to process personal data at least one of the following conditions must be met:

1. The data subject has given their consent;
2. The processing is required to carry out the functions of a professional examination and membership body;
3. It is necessary due to a legal or regulatory obligation;
4. It is necessary to protect someone's vital interests;
5. It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the AIA;
6. It is necessary for the legitimate interests of the AIA or a relevant third party and does not interfere with the rights and freedoms of the data subject.

All processing of personal data carried out by the AIA must meet one or more of the conditions above. Data is only stored to meet the legitimate interests of the AIA as detailed in Appendix 1, and may be stored securely in the AIA's database (Microsoft Dynamics) and/or on the AIA secure servers. Hardcopy forms, such as, application, membership renewal, subscription and reinstatement forms are securely stored until they are added to the database and the hardcopy form destroyed via a confidential waste contractor. See AIA Risk Management and Disaster Recovery Procedures for further information.

The date and method of consent is recorded on the database under the individuals record.

7.0 Individual Rights

GDPR gives individuals the right to access personal information held about them by AIA. The purpose of a subject access request is to allow individuals to confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary.

Individuals also have the following rights under GDPR:

- **Right to Object** – individuals can object to specific types of processing, including processing for direct marketing.
- **Right to be forgotten (erasure)** – individuals have the right to have their data erased in certain situations such as where the data are no longer required for the purpose for which they were collected, the individual withdraws consent or the information is being processed unlawfully. AIA may issue an exemption to this if the individual is or has been subject to disciplinary action or other legislative or regulatory obligations take precedence.
- Rights in relation to automated **decision making and profiling**.
- **Right to Rectification** – the right to require a controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data are incomplete, an individual can require the controller to complete the data, or to record a supplementary statement.
- **Right to Portability** – the data subject has the right to request information about them which is provided in a structured, commonly used and machine-readable form so it can be sent to another data controller.

Individuals can request to see any information that AIA holds about them which includes copies of correspondence referring to them or opinions expressed about them. However, information may be redacted or otherwise removed from a response if it includes:

- Personal information relating to other individuals (unless their permission has been obtained to release it);
- Confidential information relating to AIA's business practices;
- Information relating to examination results beyond the pass/fail result;
- Intellectual property;
- Information relating to decisions reached by the Council or committees of the Council e.g. disciplinary functions.

AIA will respond to all requests for personal information within 30 days. Depending on the complexity of the request, AIA may charge an administration fee of £10.00 per request.

A data request can only be made by the individual that it concerns. Individuals seeking access requests must contact The Data Protection Officer, AIA, Staithes 3, The Watermark, Metro Riverside, Newcastle Upon Tyne, NE11 9SN, United Kingdom, Tel. +44 (0)191 4930277 or
E: data.protection@aiaworldwide.com.

The following information must be included with the request:

- Full name and date of birth
- Preferred contact details
- Membership number, if applicable
- If a previous student or member, the year of admission.

A full description of the information requested, providing as much information as possible to help AIA locate the information such as the time periods concerned, route to membership or study provider. It may be necessary for AIA to seek further clarification if we do not have enough detail to enable us to find the information being sought.

8.0 Law Enforcement Request and Disclosure

In accordance with current legislation AIA will share an individual's data for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the prevention of financial crime, terrorist financing and anti-money laundering.

9.0 Data Retention

Individual departments are responsible for ensuring the appropriate retention periods for the information they hold and manage, based on AIA guidance (see Appendix 2).

Retention periods are set based on legal and regulatory requirements, legitimate business interests, the needs of the individual and good practice guidance.

Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. Once information is no longer needed it should be disposed of securely. Paper records should be shredded or disposed of in confidential waste facilities and electronic records should be permanently deleted.

If data is fully anonymised then there are no time limits on storage.

10.0 Membership Data

In general, membership records will be kept only for as long as is necessary to:

- fulfil and discharge the contractual obligations established between the AIA and the member, including the completion of any disciplinary action;
- provide information on the academic career and achievements of the member to employers, licensing/regulatory bodies and other organisations, as well as to the member as part of their lifelong learning record; and
- record the activities of the member as an individual and as a consumer of membership support and fulfil the obligations of the AIA to its regulators and other stakeholders.

11.0 Financial Information

Obtaining and using financial information for payments and processing is necessary to perform the AIA's duties and obligations as an organisation and how AIA handles, stores and uses financial information is set out in detail in the *AIA Information Security Policy*.

12.0 Third Parties and Suppliers

Certain conditions need to be met before personal data can be shared with a third party or before an external data processor is used to process data on behalf of the AIA.

As a rule, only specific personal data required to fulfil the process will be passed on to third parties and suppliers and must also meet the terms below:

- Any transfers of personal data must meet the data processing principles, it must be lawful and fair to the data subjects concerned.

- It must meet one of the conditions of processing. For example, legitimate reasons for transferring data would include, that there is a legal requirement or that it is necessary for the official business of the AIA.
- If no other conditions are met then consent must be obtained from the individuals concerned and appropriate privacy notices provided.
- The AIA is satisfied that the third party will meet all the requirements of GDPR particularly in terms of holding the information securely.
- Where a third party is processing personal data on behalf of the AIA a written contract must be in place.

13.0 Direct Marketing

Direct marketing relates to communication (regardless of media) with respect to advertising or marketing material that is directed to individuals e.g. mail shots, advertising courses, sector specific products or services etc. AIA makes clear opt-out provision and individuals are given the opportunity to remove themselves from lists or databases used for direct marketing purposes. AIA ceases direct marketing activity if an individual requests the marketing to stop.

14.0 Impact of Non-Compliance

All AIA staff are required to comply with this Data Protection Policy, its supporting guidance and the requirements specified in the GDPR. Any member of staff who is found to have made an unauthorised disclosure of personal information or breached the terms of this Policy may be subject to disciplinary action.

15.0 Roles and Responsibilities

As the AIA processes 'personal data' of staff, members and other individuals, it is defined as a Data Controller for the purposes of the GDPR. The Data Protection Officer (DPO) is responsible for ensuring AIA's compliance with the GDPR, for overseeing the data processing and the monitoring, revision and updating of this policy document on an annual basis or sooner, should the need arise.

The Data Protection Officer's responsibilities include:

- ensuring that the policy is produced and kept up to date
- ensuring that the appropriate practice and procedures are adopted and followed by the AIA
- providing advice and support on data protection issues within the organisation
- working collaboratively with department heads to help set the standard of data protection training for staff
- ensuring compliance with individual rights, including subject access requests
- acting as a central point of contact on data protection issues within the organisation.
- implementing an effective framework for the management of data protection
- ensuring the security measures are effective and the process is regularly tested, assessed and evaluated

In the first instance all enquiries or requests for further information or guidance relating to data protection should be addressed the AIA Data Protection Officer, AIA, Staithes 3, The Watermark, Metro Riverside, Newcastle Upon Tyne, NE11 9SN, E: data.protection@aiaworldwide.com or T: +44(0) 191 493 0277.

16.0 Appendices

Appendix 1: Assessment of Legitimate Interests

Categorisation	How to use your Data	Our Reasons
AIA Members	To deliver membership products and services To manage payments and subscriptions To detect, investigate, report, and seek to prevent financial crime. To manage risk To develop and carry out our marketing activities To obey laws and regulations applicable to AIA To respond to complaints and seek to resolve them. To provide confirmation of membership to regulators and other supervisory or professional bodies.	Fulfilling our functions as a recognised professional qualifying and membership body Our legitimate business interests Our legal duty
AIA Students	To deliver student products and services To manage payments and subscriptions To detect, investigate, report, and seek to prevent financial crime To manage risk To develop and carry out our marketing activities To obey laws and regulations applicable to AIA	Fulfilling our functions as a recognised professional qualifying and membership body Our legitimate business interests Our legal duty

	To provide information to regulators To provide confirmation of academic achievement To monitor and record work experience and academic achievement	
Lapsed Members and Students	To provide data to regulatory authorities To maintain a record of academic achievement To comply with disciplinary regulations	Fulfilling our functions as a recognised professional qualifying and membership body Our legitimate business interests Our legal duty
Academics	To deliver products and services relating to Academic Membership To manage payments and subscriptions To manage risk To develop and carry out marketing activities. To obey laws and regulations applicable to AIA. To provide information to regulators.	Fulfilling our functions as a recognised professional qualifying and membership body Our legitimate business interests Our legal duty
General Contacts and Suppliers	To develop and manage our brands, qualifications and services To manage payments To test new products To manage how we work with other companies that provide services to us and our customers Defining types of customers	Fulfilling our functions as a recognised professional qualifying and membership body Our legitimate business interests Our legal duty Consent
Potential Students and Members	To develop and manage our brands, qualifications and services	Fulfilling our functions as a recognised professional qualifying and membership body

	To deliver products and services relating to Academic Membership To manage payments and subscriptions	Our legitimate business interests
AIA Employees	Meet employment obligations	Our legitimate business interests

Appendix 2: Retention of Information

How long AIA keeps Personal Information

AIA keeps personal information for as long as individuals remain members of the AIA. After

individuals stop being a member, data may be kept for up to 10 years for one of the following reasons:

- To respond to any questions or complaints
- To show that we treated you fairly
- To maintain records according to rules that apply to us

AIA may keep data for longer than 10 years if it cannot be deleted for legal, regulatory or technical reasons.

Categorisation	Retention Period	Our Reasons
AIA Members	Lifetime, until death or opt-out and subject to regulatory requirements	To obey laws and regulations applicable to AIA. To provide information to regulators. To comply with disciplinary regulations To provide confirmation of achievement to academic institutions
AIA Students	Lifetime, until death or opt-out and subject to regulatory requirements	To obey laws and regulations applicable to AIA. To provide information to regulators. To comply with disciplinary regulations

		To provide confirmation of achievement to academic institutions
Lapsed Members and Students	Lifetime, until death or opt-out and subject to regulatory requirements	To obey laws and regulations applicable to AIA. To provide information to regulators. To comply with disciplinary regulations To provide confirmation of achievement to academic institutions
Academics	Lifetime, until death or opt-out and subject to regulatory requirements	To obey laws and regulations applicable to AIA To provide information to regulators To comply with disciplinary regulations To provide confirmation of achievement to academic institutions
General Contacts and Suppliers	Lifetime of the relationship: subject to review, opt out or regulatory requirements	To deliver our products and services To develop and manage our brands, products and services To manage payments To maintain effective financial reports on the current and previous years
Potential Students and Members	Maximum period of 12 months or until opt-out	To keep our records up to date and to provide information relating to relevant products and services Developing products and services Defining types of customers for new products or services

AIA Employees	In line with current UK employment legislation	To keep our records up to date Provide reference information for prospective employers

Appendix 3: Privacy Policy

The Association of International Accountants (AIA) is committed to protecting and respecting your privacy. We handle your personal data with integrity and confidentiality, ensuring appropriate security measures are in place.

This policy together sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it.

For the purpose of the Data Protection Act 1998 (the Act), the data controller is the Association of International Accountants of Staithes 3, The Watermark, Metro Riverside, Newcastle upon Tyne, NE11 9SN, United Kingdom.

Information we may Collect from You

We may collect and process the following data about you:

- Information that you provide by filling in forms on our site www.aiaworldwide.com. This includes information provided at the time of subscribing to our membership, posting material while using our services or requesting further services. We may also ask you for information if you report a problem with our site or services.
- If you contact us, we may keep a record of that correspondence.
- We may also ask you to complete surveys that we use for research purposes, although you do not have to respond to them.
- Details of transactions you carry out through our site and of the fulfilment of your orders.
- Details of your visits to our site including, but not limited to, traffic data, location data and other communication data.

IP Addresses

We may collect information about your computer, including where available your IP address, operating system and browser type, for system administration. This is statistical data about our users' browsing actions and patterns, and does not identify any individual.

Cookies

Our website uses cookies to distinguish you from other users of our website. This helps us to provide you with a bespoke experience when you browse our website and allows us to improve our site.

Where we Store your Personal Data

The data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Such staff maybe engaged in, among other things, the fulfilment of your order, the processing of your payment details and the provision of support services. By submitting

your personal data, you agree to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy.

All information you provide to us is stored on our secure servers. Any payment transactions will be encrypted. Where we have given you a password which enables you to access certain parts of our site, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

Uses Made of the Information

We use information held about you in the following ways:

- To ensure that content from our site is presented in the most effective manner for you and for your computer.
- To provide you with information, products or services that you request from us or which we feel may interest you, where you have consented to be contacted for such purposes.
- To carry out our obligations arising from any contracts entered between you and us.
- To notify you about changes to our service.

If you do not want us to use your data in this way, please follow the instructions outlined on the manage your e-communications form (www.aiaworldwide.com/manage-your-e-communications).

Disclosure of your Information

We may disclose your personal information to any member of our association as defined in section 1159 of the UK Companies Act 2006.

We may disclose your personal information to third parties:

- If we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets.
- If the Association of International Accountants assets are acquired by a third party, in which case personal data held by it about its members will be one of the transferred assets.
- If we are under a duty to disclose or share your personal data to comply with any legal obligation, or to enforce or apply our terms and conditions and other agreements; or to protect the rights, property, or safety of the Association of International Accountants, our members, or others.

This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

Your Rights

You have the right to ask us not to process your personal data for marketing purposes. We will usually inform you (before collecting your data) if we intend to use your data for such purposes or if we intend to disclose your information to any third party for such purposes. You can exercise your right to prevent such processing by checking certain boxes on the forms we use to collect your data. You can also

exercise the right at any time by contacting us at Staithes 3, The Watermark, Metro Riverside, Newcastle upon Tyne, NE11 9SN, United Kingdom or by email at newsdesk@aiaworldwide.com.

Our site contains links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

Access to Information

You have the right to access information held about you. Your right of access can be exercised in accordance by written or verbal request to the Association of International Accountants. Any access request will be dealt with in accordance with the GDPR policy (Section 7: Individual Rights).

Changes to our Privacy Policy

Any changes we may make to our privacy policy in the future will be posted on this page and, where appropriate, notified to you by a clear notice on our site.

Contact

Questions, comments and requests regarding this privacy policy are welcomed and should be addressed to Association of International Accountants of Staithes 3, The Watermark, Metro Riverside, Newcastle upon Tyne, NE11 9SN, United Kingdom.

Appendix 4: Sharing Information

We may share your personal information within the AIA branch network and with our partners who enable us to fulfil our function as a professional accountancy and membership organisation, including, but not limited to:

- Banks and building societies
- Insurance companies
- Study providers and examination venues
- AIA authorised advisors and inspectors
- Agents and advisers who you use to help run your accounts and services
- HM Revenue & Customs, regulators and other authorities
- Credit reference agencies
- Police and fraud prevention agencies
- Any party linked with you or your business's product or service
- Companies we have a joint venture or agreement to co-operate with
- Companies you ask us to share your data with

Appendix 5: Opt-Out Procedures

Each member of staff is responsible for ensuring that opt-out requests are managed in an efficient manner and in line with the GDPR policy.

Requests for Information / The Right to be Forgotten

The Data Protection Officer is responsible for handling all requests for personal data information. On receipt of a request the following procedures apply:

- Acknowledge receipt of the request and file the request to the relevant database record.
- If the request relates to a member or student or a lapsed member or student, the request must be considered and agreed by the Head of Membership Services and Head of Compliance and Regulation to ensure AIA's ongoing compliance with regulatory requirements and appropriate legislation.
- If granted, the information will be dispatched within 30 days.
- If rejected, an explanation of the considerations and relevant exemption(s) will be provided within 30 days.

Requests for Changes to Communication Channels

Changes to which AIA communications are received, including the AIA e-News, In Practice, International Accountant magazine, membership notifications and third-party mailings can be managed by contacting AIA, or directly through My AIA online.

If an opt-in/opt-out request is made by email or telephone it should be forwarded to the AIA Marketing Department who will action the request within 10 working days.

Changes to Individual Data

Requests to amend an individual's data held by AIA can be actioned by all AIA staff and should be done so within 10 working days.

Potential Students / Members

Enquiries for membership will be stored under and 'Enquiry' grade on the database which is searchable by date and will be removed either by opt-out or 12 months from the date of enquiry by the AIA Development Team.