Introduction

This privacy policy tells you what to expect when Assure Integrity (AI) Ltd collects personal information. The policy is a public declaration of how AI applies the data protection principles and rights afforded to individuals by the General Data Protection Regulations (GDPR) to the personal data that we process. AI is committed to complying with the 6 principles relating to the processing of personal data under the GDPR in all that we do. These principles are:

1. Lawfulness, fairness & transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality

How we collect your information

We may collect your personal data in a number of ways, for example:

- From your organisation/employer who may provide your personal data as part of an investigation or consultancy project that we are engaged to conduct.
- When you communicate with us by telephone, email or via our website, for example to make enquiries or raise concerns.
- In various other ways as you interact with us during your time as a learner at AI, for the various purposes set out below.

The types of information we collect

We may collect the following types of information from you:

- Your name, and contact information such as address, organisation, email address and telephone number, as well as your date of birth, gender, emergency contact details, national insurance number (or other tax identification number) and your passport number or national identity card details, country of domicile, your nationality and when providing work seeking opportunities, your CV.

How we use your information

Visitors to our website

When someone visits www.assureintegrity.com we use Google Analytics, to collect standard internet log information and details of visitor behaviour patterns. We do this to establish statistics such as the number of visitors to the various parts of the site. This information is only processed in a way which does not identify anyone. We do not make, and nor do we knowingly allow Google to make, any attempt to establish the identities of those visiting our website. If we do want to collect personally identifiable information through our website, we will be transparent about this and will make it clear when we collect personal information and will explain what we intend to do with it.

Use of cookies

Refer to our Cookies Statement.

Links to external websites

Some pages of our websites may contain links to websites that are not linked to this policy. If you submit your personal information to any of these third-party sites, your personal information is governed by their privacy policies. As a safety measure, we recommend that you not share any personal information with these third parties unless you've checked their privacy policies and assured yourself of their privacy practices.

Social Media Widgets

Our website may include social media widgets such as Facebook "like" buttons and Twitter "tweet" buttons that let you share articles and other information. These widgets may collect information such as your IP address and the pages you navigate in the website and may set a cookie to enable the widgets to function properly. Your interactions with these widgets are governed by the privacy policies of the companies providing them.

The lawful basis for processing your information and how we use it

We may process your personal data provided a legitimate business interest with your organisation / employer or with you exists, or in order to meet our contractual obligations in respect of the aforementioned. Accordingly, we may use your personal data for the following purposes:

- To interact with you prior to the commencement or during an investigation or consultancy project.
- To deal with any concerns or feedback you may have.
- For any other purpose for which you provide us with your personal data.

We may also process your personal data because it is necessary for the performance of our tasks carried out in the public interest or because it is necessary for our or a third party's legitimate interest. In this respect, we may use your personal data for the following:

- To monitor and evaluate the performance and effectiveness of AI, including by training our staff or monitoring their performance.
- To maintain and improve the educational, corporate, financial, estate and human resource management of AI.
- To promote equality, diversity and inclusion within AI and within the environments and partners we work with.
- To seek advice on our rights and obligations, such as where we require our own legal advice.
- To meet our compliance and regulatory obligations, such as compliance with anti-money laundering laws and safeguarding requirements.
- It is necessary for medical purposes (e.g., medical diagnosis, provision of health or social care or treatment, or a contract with a health professional).
- It is necessary to protect your or another person's vital interests, or we have your specific or, where necessary, explicit consent to do so.

Sharing your information with others

For the purposes referred to in this policy and relying on the basis for processing as set out above, we may share your personal data with third parties unless an 'opt-out' is in place. Accordingly, we may disclose limited personal data to third parties including:

- Details of our employees, our consultants, agents or clients where a legitimate reason exists for their receiving the information.

- Professional and regulatory bodies (e.g., Skills for Justice, Chartered Society of Forensic Sciences or UK's National Accreditation Body etc) in relation to the confirmation of qualifications, professional registration and conduct and the accreditation of courses Government departments and agencies where we have a statutory obligation to provide information (e.g., HSE, the Home Office (in connection with UK visas and immigration).
- Crime prevention or detection agencies (e.g., Home Office Police, the Department for Work and Pensions and Trading Standards).
- Parents, guardians, and next-of-kin (where there is a legitimate reason for disclosure).

Data transfers outside of the European Economic Area (EEA)/European Union (EU) and data portability

Information that we collect may be stored, processed and transferred between any of the countries in which we operate in or supply from in order to enable us to use the information in accordance with this policy. International transfers outside of the EEA/EU, will be managed under a Privacy Shield agreement or via other adequate security assessments and data protection controls (including EU model clauses) to enable us to carry out our service obligations to our clients, suppliers and business partners.

How long is your information retained

Subject to any other notices that we may provide to you at the time of collecting your data, we may retain your personal data for a period of seven years after your association with us has come to an end.

Security of your personal information

We use Microsoft Office 365 as our email client and we host our Quality Management System within SharePoint where some of your personal information may also be held. Office 365 provides the highest levels of security including encryption, password protection and two-factor authentication. Further information in relation to Office 365 data protection and privacy can be found here: https://www.microsoft.com/en-us/trust-center/privacy

ASSURE INTEGRITY

Your rights

If you are in the European Economic Area (EEA), you have the following rights with respect to information that AI holds about you. AI undertakes to provide you the same rights no matter where you choose to live.

Right to access: You have the right to access (and obtain a copy of, if required) the categories of personal information that we hold about you, including the information's source, purpose and period of processing, and the persons to whom the information is shared.

Right to rectification: You have the right to update the information we hold about you or to rectify any inaccuracies. Based on the purpose for which we use your information, you can instruct us to add supplemental information about you in our database.

Right to erasure: You have the right to request that we delete your personal information in certain circumstances, such as when it is no longer necessary for the purpose for which it was originally collected.

Right to restriction of processing: You may also have the right to request to restrict the use of your information in certain circumstances, such as when you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Right to data portability: You have the right to transfer your information to a third party in a structured, commonly used and machine-readable format, in circumstances where the information is processed with your consent or by automated means.

Right to object: You have the right to object to the use of your information in certain circumstances, such as the use of your personal information for direct marketing.

Right to complain: You have the right to complain to the appropriate supervisory authority if you have any grievance against the way we collect, use or share your information. This right may not be available to you if there is no supervisory authority dealing with data protection in your country.

More information in relation to these rights and a guide to the GDPR can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Making a complaint or query

AI makes every effort to meet the highest standards when collecting and using personal information. Accordingly, any complaints we receive are deemed to be extremely serious and are therefore dealt with expeditiously.

We encourage individuals and organisations alike to challenge us where it is considered we fall short of fulfilling our duties for the collection, retention and use of information or where we are

believed to be misleading or inappropriate in our application of this policy. This policy was created with brevity and clarity in mind and therefore does not provide exhaustive detail of all aspects of AI's compliance with the GDPR. Notwithstanding this, we are happy to provide clarity and additional if required. Any such requests should be made as detailed below.

How to make a complaint

If you wish to make a complaint or query about the way we have processed your personal information, please contact the Data Protection Officer using the details in the next section.

Alternatively, if you are unhappy with our response, you have the right to complain to the

Information Commissioner's Office (ICO): https://ico.org.uk/make-a-complaint/

Subject Access Requests

You may instruct us to provide you with any personal information we hold about you. Provision of such information will be subject to:

- The supply of appropriate evidence of your identity (for this purpose, we will usually accept a photocopy of your passport certified by a solicitor or bank plus an original copy of a utility bill showing your current address).
- The description of the exact information you are seeking.

AI will work collaboratively with anyone seeking access to personal data provided that we fulfil our legal obligations under the Data Protection Act 2018 and GDPR. Consequently, it may be the case where we may withhold such personal information to the extent permitted by law.

How to contact us

If you want to request information about our privacy policy, if you have a complaint or wish to execute a right, you can contact us by emailing: contact@assureintegrity.com