



GOVERNANCE / ASSURANCE / OVERSIGHT

Privacy Policy

How we handle business, enquiry and engagement information.

Effective date: 14 October 2026 | Version 1.0

1. Who we are

AI Diligence Limited (referred to as “we”, “us” or “our”) provides AI governance, review, implementation support and ongoing oversight services to organisations. We are based in the United Kingdom.

For privacy queries or requests about your personal information, please contact us using the enquiry form on our website at aidiligence.co.uk.

2. Scope and our role

This notice explains how we use personal information when you visit our website, enquire about our services, act as a client or supplier contact, or participate in our work. For those activities, we normally act as a data controller.

When a client grants us access to personal information held within its systems, or supplies personal information for an AI assessment, we may instead act as a data processor on that client’s documented instructions. In such cases the client remains the controller, and an appropriate data processing agreement will apply where required. Some engagements may involve separate controller responsibilities; these will be agreed in writing.

3. What information we may collect

- Names, job titles, employer or organisation names, work email addresses, telephone numbers and business correspondence.
- Information in website enquiries, meetings, proposals, contracts, invoices, call notes and service feedback.
- Details of AI systems and technology suppliers, user lists, access roles, policies, risk records, system configurations, workflow descriptions and audit evidence.
- Where needed for an agreed engagement: samples of AI prompts and outputs, documents, system logs or other records that may contain employee, customer, client or supplier personal information.
- Basic website technical data, such as IP address, device and browser details and security logs, where collected by our hosting providers.

4. How and why we use information

We use information to respond to enquiries, provide and manage contracted services, arrange meetings, review AI use, assess controls and risks, prepare reports and recommendations, maintain an appropriate audit trail, administer invoices, protect our systems and meet legal obligations. Where permitted, we may contact relevant business contacts about related services; you can object to direct marketing at any time.

Our lawful bases, depending on the activity, are contract (or steps before entering one), legitimate interests in operating, securing and developing our business and providing B2B services, legal obligation, and consent where it is required. We undertake balancing assessments for reliance on legitimate interests as appropriate. We do not rely on consent for every form of processing.

5. Access to client systems and confidential information

Our work may involve access to third-party software, AI platforms, Microsoft 365 environments, accounting and finance systems, client files and related records. Access should be limited to what is necessary for the agreed scope and, where practical, provided through named, permission-controlled accounts.

We may need to record the names of users, software suppliers, clients or connected companies in inventories and findings. We will aim to minimise data captured in reports and use samples or redaction where appropriate. Please do not send sensitive personal information or confidential client documents through our general website enquiry form. Use an agreed secure route instead.

6. Use of AI and other technology in our work

We may use approved business software, cloud services and AI-enabled tools to assist with administration, analysis, drafting or review. We remain responsible for handling personal data appropriately within our own role. We will not intentionally upload identifiable confidential client material or personal information to public or consumer AI services for unrestricted reuse or model training without an appropriate lawful basis, contractual safeguards and, where relevant, the client's prior agreement.

The specific systems and processors used for an engagement, permitted processing activities and any restrictions on use of client information should be recorded in the proposal, engagement terms or data processing agreement. We do not guarantee that all AI services process information in the UK.

7. Who may receive information

We may share relevant information with authorised personnel, professional advisers, insurers, IT and hosting providers, secure file storage and communications providers, and other processors necessary to deliver our services. We may also disclose information where legally required. We do not sell personal information.

Where personal data is transferred outside the UK, we will assess the transfer and use a recognised UK adequacy mechanism or appropriate safeguards where required.

8. Security and retention

We use proportionate organisational and technical safeguards, including restricted access, confidentiality expectations and secure handling practices. No transmission or storage system is completely risk-free.

We retain enquiry, contract, project and financial records for as long as reasonably necessary for the original purposes, legal compliance, professional accountability and the establishment or defence of claims. Our standard retention periods and any engagement-specific deletion or return arrangements will be documented internally and, where relevant, contractually. We will not retain engagement data indefinitely merely because we may find it useful.

9. Your rights

Depending on the circumstances, UK data protection law gives you rights to request access, correction, erasure, restriction, portability and objection, and rights relating to certain automated decisions. Not all rights apply in every case. Contact us using the details in section 1. If information is held by us only as a processor for a client, we may refer your request to that client.

You may complain to the Information Commissioner's Office (ICO) at ico.org.uk. We would appreciate the opportunity to resolve your concern first.

10. Cookies and changes

Our website may use technically necessary storage or cookies for operation and security. If non-essential analytics, advertising cookies or other tracking is introduced, we will update this notice and implement the appropriate consent controls before use.

We may amend this notice to reflect changes to law, our services or systems. The latest version should be available on our website.