obsidian

Privacy Policy

OBSIDIAN TECHNOLOGIES LIMITED

Last updated: 1 April 2026

30 CHURCHILL PLACE, CANARY WHARF, LONDON, E14 5RE

Privacy Policy

Last updated: 1 April 2026

Obsidian Technologies Limited ("Obsidian," "We," "Us," or "Our") respects your privacy and is committed to protecting your personal data. This Privacy Policy explains how Obsidian, a UK-based company, collects, uses, and discloses personal information when you visit Our website www.obsidianos.com (the "Website") and use Our services (the "Services"). It also describes your choices regarding use, access, and correction of personal data.

1. Who We Are

Obsidian Technologies Limited (doing business as Obsidian) is a company registered in England and Wales (company number 16326982), with its registered office at 30 Churchill Place, Canary Wharf, London, England, E14 5RE, United Kingdom. We provide AI-powered practice management software and related technology services to financial advisers, Independent Financial Advisers ("IFAs"), and financial advisory firms in the United Kingdom. Our platform enables advisers to automate workflows, manage client relationships, and leverage artificial intelligence technologies including AI meeting notes, document digitisation, and portfolio aggregation.

2. Scope Of This Privacy Policy

This Privacy Policy applies to personal information We collect or process when you:

- Visit or interact with Our Website.
- Use or enquire about Our Services.
- Communicate with Us by phone, email, or other methods.

Because Our primary business is B2B (business-to-business), in many instances We process personal data on behalf of Our clients (financial advisory firms and IFAs). In those scenarios, Our clients control the data, and We act as a "data processor" as defined under UK data protection laws. Where We decide how and why personal information is processed, We act as a "data controller" as defined under UK data protection laws.

3. Information We Collect

3.1 Information You Provide To Us

- **Contact Information:** Such as name, business email address, business phone number, and company name when you contact us via Our Website, sign up for Our Services, or join Our mailing list.
- **Account Information:** If you or your firm register for Our Services, We may collect login credentials (usernames, passwords) and any information you choose to provide within your account profile.
- **Communications:** If you contact Us directly (e.g., through email or phone), We will receive your name, contact details, and any other information you choose to include in your message.

3.2 Information We Collect Automatically

- **Device and Usage Information:** We may automatically collect certain information about how you use Our Website, including IP address, browser type, operating system, referring URLs, pages viewed, and other usage information.
- **Cookies and Similar Technologies:** We use cookies and similar tracking technologies to collect information about your interactions with Our Website. For full details of the specific cookies and tags We use, please see Section 13 (Cookies and Similar Technologies).

You can manage your cookie preferences via your browser settings or by visiting Our Cookie Preferences page.

3.3 Information Collected Through Our AI Features

When you use Our AI-powered features, such as AI meeting notes, document digitisation, or AI search, We may process audio recordings, meeting transcripts, uploaded documents, and related content to deliver the requested functionality.

All such AI processing, including any automated transcription of audio into text, takes place on Amazon Web Services ("AWS") infrastructure located exclusively within AWS European Union (EU) Regions. Obsidian stores Your prompts, outputs, and related content on Our platform so that You and Your firm can access, review, and manage them as part of the Service. However, this data is not retained or logged by any third-party foundation model provider, is not shared with the underlying model providers outside of the inference request itself, and is never used to train Obsidian's AI models or any third-party AI models.

3.4 Information Processed On Behalf Of Clients

When providing Our Services to financial advisory firms and IFAs, We may process personal data about their end clients and employees. This includes client names, contact details, financial information, portfolio data, and any other data uploaded to or generated within the platform. In this context, We act as a data processor, processing information solely on behalf of and under the instructions of Our clients (the data controller).

3.5 Information From Third-Party Integrations You Connect

Our platform allows You and Your firm to connect third-party services to enhance the functionality of the Service — for example, calendar, email, communication, customer relationship management (CRM), document storage, portfolio aggregation, and other financial-data providers. When You authorise such a connection (typically via OAuth or a similar delegated-authorisation mechanism), We receive and process data from the connected service only to the extent necessary to deliver the integration, and only within the scope of the permissions You granted at the point of connection. You can revoke access to any integration at any time through Your account settings, and You can request a list of currently supported integrations from Our Privacy Officer.

4. How We Use Your Information

We use the information We collect for the following purposes:

1. **To Provide and Improve Our Services:** Including setting up user accounts, providing customer support, delivering AI-powered features (such as meeting summaries, document digitisation, and portfolio aggregation), and enhancing or personalising the functionality of Our platform. A limited number of authorised Obsidian personnel may access Customer Data on a need-to-know basis where necessary to provide support, investigate and resolve issues, and improve the Services.
2. **To Communicate With You:** Responding to enquiries, sharing information about Our Services, and providing important updates and administrative messages.
3. **For Direct Marketing:** Where lawful, We may send marketing emails to business contacts about Our Services. You can unsubscribe at any time using the link provided in every marketing email.
4. **For Business Operations and Analytics:** Monitoring and analysing usage, trends, and activities in connection with Our Website and Services to improve Our offerings.
5. **Legal Compliance and Security:** Complying with applicable laws and regulations (including Financial Conduct Authority requirements where applicable), and protecting Our rights, privacy, safety, or property (and that of Our users and the public).

No Automated Decision-Making With Significant Effects. While Our Services use artificial intelligence to generate insights, summaries, and suggested content, AI outputs are made available to the adviser for review before any legally or similarly significant action is taken on the basis of them. AI features are either configured or directly invoked by the adviser, and the adviser remains responsible for how AI-generated content is used with their end clients. We do not use AI to make decisions that have legal or similarly significant effects on individuals without meaningful human involvement, within the meaning of Article 22 of the UK GDPR.

When We process data on behalf of Our clients, We do so in accordance with Our contractual obligations and the instructions provided by Our clients.

5. Legal Basis for Processing (UK/EU Visitors)

Where the UK General Data Protection Regulation (UK GDPR) or EU General Data Protection Regulation (EU GDPR) applies, We rely on the following legal bases:

- **Contractual Necessity:** Where processing is necessary to provide you (or your firm) with Our Services or to take steps at your request prior to entering into a contract.
- **Legitimate Interests:** Where processing is in Our legitimate interests, for example, to improve and secure Our Services, to send business-to-business marketing to professional contacts, and such interests are not overridden by your data protection interests or fundamental rights.
- **Consent:** For non-essential cookies and marketing communications to individuals where consent is required (including under the Privacy and Electronic Communications Regulations 2003 ("PECR")). You can withdraw consent at any time.
- **Legal Obligations:** Where processing is required to comply with a legal obligation (e.g., regulatory record-keeping or financial reporting requirements).

6. Disclosure of Your Information

We may share your personal data in the following circumstances:

- **Service Providers and Subprocessors:** With third-party vendors who process data on Our behalf and under Our instructions. Categories include Our cloud infrastructure provider (AWS), transcription and AI services, email and messaging providers, error monitoring and logging services, and third-party integrations You or Your firm have chosen to connect (see Section 3.5). A current list of Our subprocessors is available on request from Our Privacy Officer using the contact details in Section 16.
- **Corporate Transactions:** In connection with a merger, acquisition, or sale of all or a portion of Our assets, subject to appropriate confidentiality measures.
- **Legal Requirements:** When We believe disclosure is necessary to comply with the law, enforce Our contracts, protect Our rights, or respond to lawful requests from public authorities (including the Financial Conduct Authority or the Information Commissioner's Office).
- **With Your Consent:** When We otherwise have your consent to share the information.

When acting as a data processor on behalf of Our clients, We share personal data only in accordance with the client's instructions, Our Data Processing Agreement, or as required by law. A copy of Our Data Processing Agreement is available to customers on request.

7. International Data Transfers

Obsidian is a UK-based company serving clients in the United Kingdom. All personal data processed as part of delivering the Service — including Customer Data uploaded to the platform, content processed by Our AI features, and associated backups — is stored and processed exclusively within the United Kingdom or the European Economic Area (EEA).

- **Platform and Customer Data** are hosted on AWS infrastructure in EU Regions.
- **AI processing** also takes place on AWS infrastructure in EU Regions. While Obsidian stores Your prompts and outputs on the platform so You can access them, they are not retained by any third-party foundation model provider, nor used to train any AI models.
- **Backups and disaster-recovery copies** are also held within the UK/EEA.
- **Error monitoring** — if a technical error occurs on the platform, We use a specialist error-tracking service configured to keep that diagnostic data within the UK/EEA.

Limited exceptions — website analytics and advertising. Some of the analytics and advertising measurement tools We use on Our Website (see Section 13) are operated by third-party providers and may involve the transfer of pseudonymised or hashed visitor identifiers to those providers' servers, which may be located outside the UK/EEA (typically in the United States). Where this occurs, the transfer is made subject to appropriate safeguards, including the EU-US Data Privacy Framework and Standard Contractual Clauses (SCCs), and only where You have given explicit consent via Our Cookie Preferences.

Third-party integrations You connect. When You authorise an integration under Section 3.5 (for example, Google, Microsoft, or a third-party financial-data or CRM provider), data flows between Our Services and that provider's own infrastructure. That provider's handling of Your data — including any transfer outside the UK/EEA — is governed by its own privacy policy and Your agreement with that provider.

8. Privacy by Design

Obsidian has adopted a formal **Privacy by Design Policy** that embeds privacy considerations into every stage of product development and service delivery. Under this policy the following principles are employed:

- **Proactive, not reactive:** Privacy risks are identified and addressed from the earliest design stages, before personal data is processed.
- **Privacy as the default:** Our Services are configured by default to collect and retain only the minimum personal data necessary for the intended purpose.
- **End-to-end security:** Personal data is protected from collection through to secure deletion, with appropriate technical and organisational controls at every stage.
- **Transparency and user control:** We provide clear information about Our data practices and give individuals meaningful control over their personal data.

Where processing is likely to result in a high risk to individuals, We conduct a **Data Protection Impact Assessment (DPIA)** before processing begins, in accordance with Article 35 of the UK GDPR.

9. Data Security

The security of Your information is important to Us. We maintain a written information security programme with appropriate administrative, physical, and technical measures designed to protect Customer Data against loss, misuse, unauthorised access, disclosure, alteration, or destruction.

Our security measures include encryption of personal data in transit and at rest, role-based access controls on the principle of least privilege, multi-factor authentication for privileged accounts, continuous monitoring and audit logging, regular security assessments, staff training on data protection and security, and formal risk management of third-party vendors. Our security policies and controls are reviewed regularly and updated as appropriate.

These measures are designed to provide a level of security appropriate to the risk of processing.

10. Data Retention

We retain personal data only for as long as is necessary to fulfil the purposes described in this Privacy Policy and to comply with Our legal, regulatory, and contractual obligations. Our approach is governed by Our internal Data Retention Policy, which is reviewed at least annually.

Indicative retention periods include:

- **Customer account data** (names, emails, login credentials, billing records): for the duration of the Customer Agreement and typically up to six (6) years thereafter, reflecting HMRC record-keeping requirements and, where the Customer is a regulated financial firm, applicable Financial Conduct Authority obligations.
- **Customer Data processed on behalf of Financial Advisory/IFA firms** (client records, meeting notes, documents): retained and deleted in accordance with the instructions of the controlling firm and the Data Processing Agreement between Us and that firm. On termination, such data is deleted or returned as directed by the controller, except where retention is required:
- in connection with a lawful request, information notice, investigation, complaint, or enforcement action by the **Financial Conduct Authority (FCA)**, the **Financial Ombudsman Service**, the **Information Commissioner's Office**, or another competent regulatory or supervisory authority;
- to comply with FCA record-keeping rules that, by contract or by law, apply to the Customer Data We hold (for example, obligations relating to suitability records, client communications, or pension-transfer advice);
- to comply with Obsidian's own legal, tax, or accounting obligations; or
- to establish, exercise, or defend legal claims.

In all such cases, only the minimum data necessary is retained, for no longer than the relevant obligation requires, and is then securely deleted.

- **Website and analytics data:** retained only for as long as relevant to the purpose for which it was collected (typically up to 26 months for analytics events), and anonymised or deleted thereafter.
- **Server and security logs:** retained for up to 90 days, with longer retention in secure archive storage where required for security monitoring or regulatory purposes.
- **Marketing records:** retained until you unsubscribe or object, and for a short period thereafter to document the withdrawal of consent.
- **Backup copies:** retained in accordance with Our internal backup retention schedule and purged once they are no longer required for recovery or disaster-continuity purposes.
- **Legal, regulatory, and dispute records:** retained where necessary to establish, exercise, or defend legal claims, respond to regulatory enquiries, or comply with legal obligations.

When personal data is no longer required, We take appropriate steps to delete or anonymise it in line with Our internal Data Retention Policy. Deletion may not always be instantaneous: residual copies may persist for a limited period in backup systems, version histories, and audit logs. In those cases, access to the residual data is restricted, and it is retained no longer than is reasonably necessary to support legitimate recovery, audit, or compliance purposes. On request, We can provide written confirmation that Your data has been deleted from Our active production systems.

11. Data Breach Notification

In the event of a personal data breach likely to result in a risk to the rights and freedoms of individuals, We will notify the Information Commissioner's Office (ICO) without undue delay and, where feasible, within **72 hours** of becoming aware of the breach, as required by Article 33 of the UK GDPR. Where the breach is likely to result in a high risk to individuals, We will also notify the affected individuals (or, where We act as a processor, Our Customer as controller) without undue delay, in line with Article 34. All breaches and near-misses are logged internally and reviewed as part of Our Incident Response Policy.

12. Your Rights

Under applicable UK and EU data protection laws, you may have the right to:

- Access and obtain a copy of your personal data.
- Request rectification or erasure of your personal data.
- Object to or request restriction of processing of your personal data, including processing for direct marketing.
- Withdraw consent where We rely on your consent to process your personal data.
- Data portability, where applicable.
- Not be subject to a decision based solely on automated processing that produces legal or similarly significant effects (see Section 4).

If you wish to exercise any of these rights or have questions about your rights, please contact Our Privacy Officer using the details in Section 16. We will consider and respond to requests in accordance with applicable data protection laws (generally within one month).

If you believe We have infringed or violated your data protection rights, you have the right to lodge a complaint with your local data protection authority. In the United Kingdom, that is the Information Commissioner's Office (ICO) at ico.org.uk.

13. Cookies and Similar Technologies

We use cookies and similar technologies to operate and improve Our Website. Categories currently in use include:

- **Strictly necessary cookies** — enable core functionality such as page navigation, session management, and remembering your display preferences. These are essential and cannot be turned off.
- **Analytics cookies** — Google Analytics 4 (configured with the EU data-residency endpoint and IP anonymisation) helps Us understand how visitors interact with Our Website. Non-essential; UK/EEA visitors are only tracked with explicit consent.
- **Advertising and social cookies** — third-party advertising and professional-network platforms We use to measure the effectiveness of Our B2B campaigns and reach relevant professional audiences. Non-essential; UK/EEA visitors are only tracked with explicit consent.
- **Tag management** — a tag management service used to deploy and manage the above tags in a controlled manner. It does not itself collect personal data beyond what is needed to load the tags You have consented to.

You can manage your cookie preferences at any time by visiting Our Cookie Preferences page. Withdrawing consent will stop future non-essential tracking but does not affect tracking that occurred before you withdrew consent.

Server-side marketing measurement. In addition to browser-based cookies, We use server-side conversion measurement provided by the advertising platforms listed above. This may involve transmitting business-contact identifiers (such as hashed email addresses) to those platforms to attribute marketing activity. We do so only in relation to professional B2B contacts, on the same lawful bases set out in Section 5, and subject to consent where required.

14. Third-Party Links

Our Website may contain links to other websites or services that We do not control. This Privacy Policy does not apply to those third-party websites. We encourage you to review the privacy policies of those third parties to understand their practices.

15. Changes To This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in Our practices, technology, legal requirements, and other factors. When We do, We will post the updated Privacy Policy on this page and update the "Last updated" date at the top. We encourage you to review this page periodically to remain informed of any changes.

16. Contact Us

If you have any questions about this Privacy Policy, wish to exercise your data protection rights, or have any other privacy-related queries, please contact Our Privacy Officer:

Ian Stone, Head of Compliance and Privacy Officer

Email: ian@obsidianos.com

Obsidian Technologies Limited

30 Churchill Place, Canary Wharf, London, England, E14 5RE

Company number: 16326982 (registered in England and Wales)

General enquiries: support@obsidianos.com

You also have the right to lodge a complaint with the Information Commissioner's Office (ICO) at ico.org.uk.