obsidian

Obsidian Technologies Limited

Data Processing Addendum

Last updated: 1 April 2026

This Data Processing Addendum ("DPA") forms part of and supplements Obsidian's Terms of Service or Terms & Conditions (the "Terms") and any other agreement governing the Customer's use of the Services (together with the Terms, the "Agreement"), entered into by and between the customer that accepts the Agreement or uses the Services (the "Customer") and Obsidian Technologies Limited, company number 16326982 (together with its Affiliates, "Obsidian"). This DPA is the data processing agreement contemplated by the Agreement and applies by default to every Customer. To the extent Obsidian processes Personal Data on the Customer's behalf, by accepting the Agreement or using the Services, the Customer enters into this DPA, which is incorporated into the Agreement by reference and takes effect on that date (the "Effective Date"), whether or not the Customer has requested or received a copy. For the avoidance of doubt, this DPA binds all Customers automatically; Obsidian publishes this agreement on its website and additionally makes a copy available to Customers on request. Any terms not defined in this DPA shall have the meaning set forth in the Agreement.

1. Definitions

1. "Authorised Subprocessor" means a third party who has a need to know or otherwise access the Customer's Personal Data to enable Obsidian to perform its obligations under this DPA or the Agreement, and who is either (1) listed in Exhibit B or (2) subsequently authorised under Section 4.2 of this DPA.
2. "Privacy Laws" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data including, each to the extent applicable: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR") and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR") (together, collectively, the "GDPR"); (ii) the UK Data Protection Act 2018 ("DPA 2018"); and (iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"), in each case, as updated, amended or replaced from time to time. The terms "controller," "Personal Data Breach," "processing," "processor," and "supervisory authority" shall have the meanings set forth for such or equivalent terms under Privacy Laws.
3. "Data Subject" means a natural person whose Personal Data is protected by Privacy Laws.
4. "Data Subject Request" means a request from a Data Subject to exercise their rights over Personal Data afforded pursuant to Privacy Laws.
5. "ex-EEA Transfer" means the transfer of Personal Data subject to the GDPR from the European Economic Area ("EEA") to a country where the transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.
6. "ex-UK Transfer" means the transfer of Personal Data subject to Chapter V of the UK GDPR from the United Kingdom ("UK") to a country, territory, sector, or international organisation where such transfer is not governed by adequacy regulations made under the UK GDPR and the DPA 2018.
7. "Personal Data" means any information provided to Obsidian by or on behalf of the Customer in connection with the Services, or that is generated or derived in the course of providing the Services, that relates to an identified or identifiable Data Subject and constitutes "personal data" or an equivalent term under Privacy Laws.
8. "Standard Contractual Clauses" means, as applicable, (i) with respect to ex-EEA Transfers, the standard contractual clauses approved by the European Commission in Commission Decision 2021/914, for transfers of personal data to countries not otherwise recognised as offering an

adequate level of protection for personal data by the European Commission (as amended and updated from time to time), as modified by Section 6 of this DPA ("EU SCCs"); and (ii) with respect to ex-UK Transfers, the EU SCCs as amended by the UK Addendum ("UK SCCs").

9. "UK Addendum" means the template International Data Transfer Addendum issued by the Information Commissioner in accordance with s119A of the Data Protection Act 2018 (as may be amended from time to time), as completed by Exhibit C.
10. "UK Adequacy Regulations" means any regulations made under the UK GDPR or the DPA 2018 specifying that a third country, territory, sector, or international organisation ensures an adequate level of protection for Personal Data (including any partial or sector-specific bridge such as the UK Extension to the EU-U.S. Data Privacy Framework).
11. "Affiliate" means, with respect to a party, any entity that directly or indirectly controls, is controlled by, or is under common control with that party, where "control" means the direct or indirect ownership of more than fifty percent of the voting securities or interests of an entity, or the power to direct or cause the direction of its management and policies.
12. "Business Contact Data" means the business contact information of the Customer's personnel and authorised users that Obsidian processes to establish, manage, and administer its business relationship with the Customer, such as names, job titles, business email addresses, business telephone numbers, and similar professional contact details.
13. "Usage Data" means data and analytics generated through, or relating to, the Customer's and its users' access to and use of the Services, including log data, device and connection information, feature usage, and performance and diagnostic data, in each case to the extent such data does not include the content of Customer Data.

2. Role of the Parties; Description of Processing

1. Except as expressly set forth in this DPA or the Agreement, with respect to Personal Data, the Customer is the Controller and Obsidian is a Processor, or to the extent the Customer is a Processor to a third-party Controller, Obsidian is a subprocessor. Custody, execution, trading, and settlement services that may be offered by Obsidian Securities Limited are not part of the Services or the Agreement (see clause 1.2 of the Terms) and are outside the scope of this DPA; any processing of Personal Data in connection with those services will be governed by the separate terms, and a separate or supplemental data processing agreement, applicable to them.
2. Obsidian shall process Personal Data only (i) for purposes set forth in the Agreement, (ii) in a manner consistent with the documented instructions provided by the Customer, which shall include the Agreement and this DPA, and (iii) as required by Privacy Laws or a supervisory authority; in such case, Obsidian shall inform the Customer of that legal requirement before processing to the extent legally permitted. The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects involved, are described in Exhibit A to this DPA. Obsidian shall, without undue delay, notify the Customer if an instruction, in Obsidian's opinion, infringes the Privacy Laws or the requirements of a supervisory authority.
3. Obsidian shall not: (i) sell or share Personal Data, or process Personal Data for any purpose other than providing the Services to the Customer pursuant to the Agreement, as instructed by the Customer, or as otherwise permitted by Privacy Laws; (ii) retain, use, or disclose Personal Data outside of Obsidian's direct business relationship with the Customer; and (iii) combine Personal Data received from, or on behalf of, the Customer with Personal Data that it receives from, or on behalf of, another party or person, except as necessary to provide the Services or as otherwise instructed

by the Customer. Obsidian shall, without undue delay, notify the Customer if it determines that it can no longer meet its obligations under Privacy Laws.

4. The Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Privacy Laws. The Customer shall ensure that the processing of Personal Data in accordance with the Customer's instructions will not cause Obsidian to be in breach of the Privacy Laws. The Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Obsidian by or on behalf of the Customer, (ii) the means by which the Customer acquired any such Personal Data, and (iii) the instructions it provides to Obsidian regarding the processing of such Personal Data. The Customer is responsible for determining the Privacy Laws applicable to its processing, including by reference to the location of the Data Subjects whose Personal Data it submits to the Services, and warrants that it has all necessary rights, consents, and lawful bases to provide such Personal Data to Obsidian and to authorise the processing contemplated by the Agreement and this DPA, including in respect of Data Subjects located outside the United Kingdom. The Customer shall not provide or make available to Obsidian any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Obsidian from all claims and losses in connection therewith.
5. **No Training of AI Models on Customer Data.** Obsidian does not, and will not, use Customer Data — including any audio, transcripts, documents, or other Personal Data submitted to, or generated by the Services on behalf of, the Customer — to train, fine-tune, or otherwise develop or improve any artificial intelligence or machine-learning models, and will procure that its Authorised Subprocessors do not do so. For clarity, Obsidian uses artificial intelligence and machine-learning models on an inference basis only, solely to deliver the Services to the Customer, and does not use Customer Data to develop or improve models or services for any other customer or third party.

3. Confidentiality

Obsidian shall ensure that any person it authorises to process Personal Data has committed to protect Personal Data in accordance with Obsidian's confidentiality obligations in the Agreement, including by being subject to an appropriate statutory or contractual duty of confidentiality. The Customer agrees that Obsidian may disclose Personal Data to its advisers, auditors, or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to the Customer.

4. Authorised Subprocessors

1. The Customer acknowledges and agrees that Obsidian may (1) engage its Affiliates and the Authorised Subprocessors listed in Exhibit B to this DPA to access and process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data. By way of this DPA, the Customer provides general written authorisation to Obsidian to engage subprocessors as necessary to perform the Services.
2. A list of Obsidian's current Authorised Subprocessors can be found at obsidianos.com/security/subprocessors (the "List"). Such List may be updated by Obsidian from time to time. Obsidian may provide a mechanism to subscribe to notifications of new Authorised Subprocessors, and Customer agrees to subscribe to such notifications where available. At least thirty days before enabling any third party other than existing Authorised Subprocessors to access

or participate in the processing of Personal Data, Obsidian will add such third party to the List and notify the Customer. The Customer may object to such an engagement by informing Obsidian within thirty days of receipt of the aforementioned notice, provided such objection is in writing and based on reasonable grounds relating to data protection. The Customer acknowledges that certain subprocessors are essential to providing the Services and that objecting to the use of a subprocessor may prevent Obsidian from offering the Services to the Customer.

3. If the Customer reasonably objects to an engagement in accordance with Section 4.2, and Obsidian cannot provide a commercially reasonable alternative within a reasonable period of time, the Customer may discontinue the use of the affected Service by providing written notice to Obsidian. Discontinuation shall not relieve the Customer of any fees owed to Obsidian under the Agreement. If the Customer does not object to the engagement of a third party in accordance with Section 4.2 within thirty days of notice by Obsidian, that third party will be deemed an Authorised Subprocessor for the purposes of this DPA.
4. Obsidian will enter into a written agreement with each Authorised Subprocessor imposing data protection obligations comparable to those imposed on Obsidian under this DPA with respect to the protection of Personal Data. Where an Authorised Subprocessor fails to fulfil its data protection obligations under such written agreement, Obsidian will remain liable to the Customer for the performance of the Authorised Subprocessor's obligations under such agreement.
5. If the Customer and Obsidian have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), (i) the above authorisations will constitute the Customer's prior written consent to the subcontracting by Obsidian of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorised Subprocessors that must be provided by Obsidian to the Customer pursuant to the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by Obsidian beforehand, and that such copies will be provided by Obsidian only upon request by the Customer.

5. Security of Personal Data

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Obsidian shall maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing Personal Data, as described on Obsidian's Trust Centre, available at: obsidianos.com/security ("Obsidian Security Page").

6. Transfers of Personal Data

1. The parties acknowledge that Obsidian's primary processing operations, including the storage and processing of Customer client data, take place within the United Kingdom (the Amazon Web Services Europe (London) Region), and that Obsidian's principal infrastructure subprocessor contracts through an entity established in the European Economic Area. Obsidian hosts Customer client data in a single region and does not replicate, back up, or store Customer client data outside the United Kingdom. Obsidian may nonetheless transfer limited Personal Data processed under this DPA outside the EEA or the UK to the extent necessary to provide the Services (for example, where an ancillary Authorised Subprocessor processes limited operational data outside the United Kingdom). If Obsidian transfers Personal Data protected under this DPA to a jurisdiction for which an applicable adequacy decision or adequacy regulations have not been issued, Obsidian will ensure

that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Privacy Laws.

2. **Transfers from the EEA.** Where Personal Data subject to the EU GDPR is transferred from the EEA to Obsidian in the United Kingdom, the parties rely on the European Commission's adequacy decision in respect of the United Kingdom (as renewed, amended, or replaced from time to time). Where such adequacy decision does not apply or ceases to be available, or where Personal Data is otherwise the subject of an ex-EEA Transfer, the EU SCCs apply and are deemed entered into (and incorporated into this DPA by this reference) and completed as set out in Section 6.4 below, as follows:
    1. Module One (Controller to Controller) of the EU SCCs applies when Obsidian is processing Personal Data as a controller pursuant to Section 11 of this DPA.
    2. Module Two (Controller to Processor) of the EU SCCs applies when the Customer is a controller and Obsidian is processing Personal Data for the Customer as a processor pursuant to Section 2 of this DPA.
    3. Module Three (Processor to Subprocessor) of the EU SCCs applies when the Customer is a processor and Obsidian is processing Personal Data on behalf of the Customer as a subprocessor.
3. **Transfers from the UK.** Where Personal Data subject to the UK GDPR is the subject of an ex-UK Transfer, the parties rely on (i) UK Adequacy Regulations where available in respect of the relevant recipient or destination (including, for transfers to organisations in the United States that are certified under the UK Extension to the EU-U.S. Data Privacy Framework, that bridge), or (ii) where UK Adequacy Regulations do not apply, the UK SCCs, which are deemed entered into and incorporated into this DPA by reference, as completed by Exhibit C.
4. For each applicable module of the EU SCCs, the following applies:
    1. The optional docking clause in Clause 7 does not apply.
    2. In Clause 9, Option 2 (general written authorisation) applies, and the minimum time period for prior notice of subprocessor changes shall be as set forth in Section 4.2 of this DPA.
    3. In Clause 11, the optional language does not apply.
    4. All square brackets in Clause 13 are hereby removed.
    5. In Clause 17 (Option 1), the EU SCCs will be governed by the law of the Republic of Ireland.
    6. In Clause 18(b), disputes will be resolved before the courts of the Republic of Ireland.
    7. Exhibit B to this DPA contains the information required in Annex I and Annex III of the EU SCCs.
    8. The Obsidian Security Page contains the information required in Annex II of the EU SCCs.
    9. By entering into this DPA, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.
5. **Supplementary Measures.** In respect of any ex-EEA Transfer or ex-UK Transfer made pursuant to the Standard Contractual Clauses, the following supplementary measures shall apply:
    1. As of the date of this DPA, Obsidian has not received any formal legal requests from any government intelligence or security service/agency in any country to which the Personal Data is being exported, for access to (or for copies of) Customer's Personal Data ("Government Agency Requests").

2. If, after the date of this DPA, Obsidian receives any Government Agency Requests, Obsidian shall attempt to redirect the law enforcement or government agency to request that data directly from the Customer. As part of this effort, Obsidian may provide the Customer's basic contact information to the government agency. If compelled to disclose the Customer's Personal Data to a law enforcement or government agency, Obsidian shall give the Customer reasonable notice of the demand and cooperate to allow the Customer to seek a protective order or other appropriate remedy unless Obsidian is legally prohibited from doing so. Obsidian shall not voluntarily disclose Personal Data to any law enforcement or government agency. The Customer and Obsidian shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in light of such Government Agency Requests.
3. The Customer and Obsidian will confer, as needed, to consider whether: (i) the protection afforded by the laws of the country of the data importer to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, whichever the case may be; (ii) additional measures are reasonably necessary to enable the transfer to be compliant with the Privacy Laws; and (iii) it is still appropriate for Personal Data to be transferred to the relevant data importer, taking into account all relevant information available to the parties, together with guidance provided by the supervisory authorities.
4. If Privacy Laws require the Customer to execute the Standard Contractual Clauses applicable to a particular transfer of Personal Data as a separate agreement, Obsidian shall, on request of the Customer, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Customer to reflect the applicable appendices and annexes, the details of the transfer, and the requirements of the relevant Privacy Laws.
5. If either (i) any of the means of legitimising transfers of Personal Data outside of the EEA or UK set forth in this DPA cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Obsidian may by notice to the Customer, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Privacy Laws.

7. Rights of Data Subjects

1. Obsidian shall, to the extent permitted by Privacy Laws, notify the Customer upon receipt of a Data Subject Request. If Obsidian receives a Data Subject Request in relation to Personal Data, Obsidian will advise the Data Subject to submit their request to the Customer, and the Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. The Customer is solely responsible for ensuring that Data Subject Requests communicated to Obsidian are valid and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.
2. Obsidian shall, at the request of the Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organisational measures to assist the Customer in complying with the Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) the Customer is itself unable to respond without Obsidian's assistance and (ii) Obsidian is able to do so in accordance with all applicable laws, rules, and regulations. The Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Obsidian.

8. Actions and Access Requests; Audits

1. Obsidian shall, taking into account the nature of the processing and the information available to Obsidian, provide the Customer with reasonable cooperation and assistance where necessary for the Customer to comply with its obligations under the Privacy Laws to conduct a data protection impact assessment and/or to demonstrate such compliance, provided that the Customer does not otherwise have access to the relevant information. The Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Obsidian.
2. Obsidian shall, taking into account the nature of the processing and the information available to Obsidian, provide the Customer with reasonable cooperation and assistance with respect to the Customer's cooperation and/or prior consultation with any supervisory authority or regulatory agency, where necessary and where required by the Privacy Laws. The Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Obsidian.
3. Obsidian shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA. Upon the Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Obsidian shall, either (i) make available for the Customer's review copies of such certifications or reports as Obsidian holds from time to time (currently including Obsidian's ISO 27001 certification) demonstrating Obsidian's compliance with prevailing data security standards applicable to the processing of the Customer's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Privacy Laws, allow the Customer's independent third-party representative to conduct an audit or inspection of Obsidian's data security infrastructure and procedures that is sufficient to demonstrate Obsidian's compliance with its obligations under Privacy Laws, provided that (a) the Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Obsidian's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to the Customer. The Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Obsidian for any time expended for on-site audits. If the Customer and Obsidian have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the audits described in the EU SCCs shall be carried out in accordance with this Section 8.3.

9. Personal Data Breach

1. In the event of a Personal Data Breach, Obsidian shall, without undue delay, inform the Customer of the Personal Data Breach and take such steps as Obsidian in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Obsidian's reasonable control).
2. In the event of a Personal Data Breach, Obsidian shall, taking into account the nature of the processing and the information available to Obsidian, provide the Customer with reasonable cooperation and assistance necessary for the Customer to comply with its obligations under the Privacy Laws with respect to notifying (i) the relevant supervisory authority or regulatory agency and (ii) Data Subjects affected by such Personal Data Breach without undue delay.
3. The obligations described in Sections 9.1 and 9.2 shall not apply in the event that a Personal Data Breach results from the actions or omissions of the Customer. Obsidian's obligation to report or

respond to a Personal Data Breach under Sections 9.1 and 9.2 will not be construed as an acknowledgement by Obsidian of any fault or liability with respect to the Personal Data Breach.

10. Return or Destruction of Personal Data

Upon the termination or expiration of the Agreement, at the Customer's choice, Obsidian shall return or delete Personal Data, unless further storage of such Personal Data is required or authorised by applicable law. If return or destruction is impracticable or prohibited by law, rule, or regulation, Obsidian shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule, or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If the Customer and Obsidian have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.1(d) and the EU SCCs (as applicable) shall be provided by Obsidian to the Customer only upon the Customer's request.

11. Obsidian's Role as a Controller

The parties acknowledge and agree that Obsidian may process Business Contact Data and Usage Data (as defined in this DPA) as an independent controller, not a joint controller with the Customer. Obsidian will process Business Contact Data and Usage Data as a controller (i) to manage the relationship with the Customer; (ii) to carry out Obsidian's core business operations, such as accounting, audits, tax preparation and filing, and compliance purposes; (iii) to monitor, investigate, prevent, and detect fraud, security incidents, and other misuse of the Services, and to prevent harm to the Customer; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Obsidian is subject; and (vi) as otherwise permitted under Privacy Laws and in accordance with this DPA and the Agreement. Obsidian may also process Usage Data as a controller to provide, optimise, and maintain the Services, to the extent permitted by Privacy Laws. Any processing by Obsidian as a controller shall be in accordance with Obsidian's privacy policy set forth at obsidianos.com/legal.

12. Conflict

In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this DPA; (3) the Agreement; and (4) Obsidian's privacy policy. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement. Except for the Standard Contractual Clauses (which are governed by the law specified in Section 6), this DPA is governed by and construed in accordance with the laws of England and Wales, consistent with the Agreement.

Exhibit A

Details of Processing

Nature and Purpose of Processing: Obsidian will process Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with the Customer's instructions as set forth in this DPA. The Services comprise Obsidian's AI practice-management platform for financial-advice firms, including capturing, recording, transcribing, and summarising meetings; customer relationship management (CRM); portfolio and account aggregation across custodians and platforms; document digitisation; AI-assisted search; and the generation of suitability reports and client communications. The nature of processing includes, without limitation:

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Holding data, including storage, organisation, and structuring
- Using data, including analysis, consultation, and testing
- Updating data, including correcting, adaptation, alteration, alignment, and combination
- Protecting data, including restricting, encrypting, and security testing
- Sharing data, including disclosure, dissemination, allowing access, or otherwise making available
- Returning data to the Customer or Data Subject
- Erasing data, including destruction and deletion

Duration of Processing: Obsidian will process Personal Data as long as required to provide the Services to the Customer or as otherwise set forth in the Agreement.

Categories of Data Subjects:

- The Customer's personnel and authorised users (including advisers, paraplanners, administrators, and other staff);
- The Customer's clients and prospective clients (i.e., the end clients of the financial-advice firm), and, where recorded by the Customer, their associated contacts, beneficiaries, and family members;
- Participants in meetings recorded or transcribed using the Services; and
- Any other Data Subject whose Personal Data the Customer chooses to input into or process through the Services.

Categories of Personal Data:

- Identity and contact details (such as names, email addresses, telephone numbers, and postal addresses);
- Professional and demographic information;
- Financial information, including portfolio holdings, account and product information, valuations, transactions, and other data aggregated from custodians and platforms;
- Meeting audio recordings, transcripts, and notes derived from them;
- Documents uploaded or digitised through the Services (which may contain a range of personal data);

- CRM records, tasks, and the content of communications and correspondence (including client-facing emails); and
- Business Contact Data, Usage Data, and any other Personal Data contained in Customer Data submitted to the Services.

Sensitive Data or Special Categories of Data: The Services are not designed or intended for the routine or systematic processing of special category data (as defined in Article 9 of the GDPR) or data relating to criminal convictions and offences. The parties acknowledge, however, that because the Services include the recording and transcription of meetings and the ingestion of documents, Personal Data submitted by Customer may incidentally contain special category data (for example, references to a Data Subject's health, or other special category data disclosed in the course of a client meeting). Obsidian processes any such data solely as part of providing the Services, in accordance with Customer's documented instructions and the security measures described on the Obsidian Security Page. Customer, as controller, is responsible for ensuring that, where such data is processed, Customer has a valid condition for processing under Article 9 of the GDPR and, where applicable, Schedule 1 of the UK Data Protection Act 2018 (including, where required, an Appropriate Policy Document), and for providing any notices and obtaining any consents required under Privacy Laws.

Exhibit B

The following includes the information required by Annex I and Annex III of the EU SCCs, and Table 1, Annex 1A, and Annex 1B of the UK Addendum.

1. The Parties

Data exporter(s): Customer

- Contact details: The account, administrative, or billing contact associated with the Customer's account for the Services, as provided by the Customer on registration or as subsequently updated by the Customer.
- Signature and date: By accepting the Agreement or using the Services, the Customer is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date.
- Role (controller/processor): The Customer's role is set forth in Section 2 of this DPA.

Data importer(s): Obsidian Technologies Limited (company number 16326982)

- Address: 30 Churchill Place, Canary Wharf, London, England, E14 5RE, United Kingdom.
- Contact details: privacy@obsidianos.com (or the privacy contact set out in Obsidian's Privacy Policy at obsidianos.com/legal).
- Signature and date: By making the Services available to Customer, Obsidian is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date.
- Role (controller/processor): Obsidian's role is set forth in Section 2 of this DPA.

2. Description of the Transfer

Data Processing Element	Description
Data Subjects	As described in Exhibit A of the DPA

Data Processing Element	Description
Categories of Personal Data	As described in Exhibit A of the DPA
Special Category Personal Data (if applicable)	As described in Exhibit A of the DPA
Nature of the Processing	As described in Exhibit A of the DPA
Purposes of Processing	As described in Exhibit A of the DPA
Duration of Processing and Retention (or the criteria to determine such period)	As described in Exhibit A of the DPA
Frequency of the transfer	As necessary to perform all obligations and rights with respect to Personal Data as provided in the Agreement or DPA
Recipients of Personal Data Transferred to the Data Importer	Obsidian's list of Subprocessors can be found at: obsidianos.com/security/subprocessors.

3. Competent Supervisory Authority

For ex-EEA Transfers, the supervisory authority shall be the supervisory authority of the data exporter, as determined in accordance with Clause 13 of the EU SCCs. The supervisory authority for the purposes of the UK Addendum shall be the UK Information Commissioner's Office.

Exhibit C

UK Addendum: International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Field	Details	
Start Date	This UK Addendum shall have the same effective date as the DPA	
The Parties	Exporter	Importer
Parties' Details	Customer	Obsidian Technologies Limited
Key Contact	See Exhibit B of this DPA	See Exhibit B of this DPA

Table 2: Selected SCCs, Modules and Selected Clauses

Field	Details
EU SCCs	The version of the Approved EU SCCs which this UK Addendum is appended to as defined in the DPA and completed by Sections 6.2 and 6.4 of the DPA.

Table 3: Appendix Information

Annex	Details
Annex 1A: List of Parties	As per Table 1 above
Annex 1B: Description of Transfer	See Exhibit B of this DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data	See the Obsidian Security Page
Annex III: List of Sub-processors (Modules 2 and 3 only)	See Exhibit B of this DPA

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Field	Selection
Ending this UK Addendum when the Approved UK Addendum changes	☒ Importer ☒ Exporter ☐ Neither Party

Part 2: Mandatory Clauses

The Mandatory Clauses of the UK Addendum are incorporated herein by reference.