Obsidian Security – Data Processing Addendum

This Data Processing Addendum ("**DPA**") supplements and is incorporated into the Agreement made by and between Obsidian and Customer.

1. **Definitions.** The definitions of certain capitalized terms used in this DPA are set forth below. Others are defined in the body of the DPA. Capitalized terms not defined in this DPA are defined in the Agreement.

   1.1. **"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

   1.2. "**Customer Personal Data**" means the Personal Data described under Schedule 1 to this DPA, in respect to which the Customer is the Controller.

   1.3. "**Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including, as applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder and the California Privacy Rights Act of 2020 (collectively, the "**CCPA/CPRA**"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**" or "**GDPR**"), (iii) the Swiss Federal Act on Data Protection ("**FADP**"), (iv) 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 (the "**UK GDPR**") and (v) the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.

   1.4. "**Data Subject**" means the identified or identifiable natural person to whom Personal Data relates.

   1.5. "**EEA**" means European Economic Area.

   1.6. "**Personal Data**" means information about an identified or identifiable natural person or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Data Protection Laws.

   1.7. "**Processing**" and inflections thereof refer to any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

   1.8. "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

   1.9. "**Restricted Transfer**" means: (i) where EU GDPR applies, a transfer of Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy determination, (ii) where UK GDPR applies, a transfer of Personal Data from the United Kingdom toany country that is not subject to an adequacy determination, or (iii) where FADP applies, a transfer of Personal Data from Switzerland to any country that is not subject to an adequacy determination.

   1.10. "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data being Processed by Obsidian.

   1.11. "**Specified Notice Period**" is 72 hours.

   1.12. "**Subprocessor**" means any third party authorized by Obsidian to Process any Customer Personal Data.

   1.13. "**Subprocessor List**" means the list of Obsidian's Subprocessors as identified below and on the Trust Portal.

   1.14. "**Trust Portal**" means https://trust.obsidiansecurity.com/.

2. Scope and Duration.

2.1. **Roles of the Parties**. This DPA applies to Obsidian as a Processor of Customer Personal Data and to Customer as a Controller or Processor of Personal Data.

2.2. **Scope of DPA**. This DPA applies to Obsidian's Processing of Customer Personal Data under the Agreement to the extent such Processing is subject to Data Protection Laws. This DPA is governed by the governing law of the Agreement unless otherwise required by Data Protection Laws.

2.3. **Duration of DPA**. This DPA commences on the start of the Initial Term and terminates upon expiration or termination of the Agreement (or, if later, the date on which Obsidian has ceased all Processing of Personal Data).

2.4. **Order of Precedence**. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) any Standard Contractual Clauses or other measures to which the Parties have agreed in Schedule 3 (Cross-Border Transfer Mechanisms) or Schedule 4 (Region-Specific Terms), (2) this DPA, and (3) the Agreement. To the fullest extent permitted by Data Protection Laws, any claims brought in connection with this DPA (including its Schedules) will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations, set forth in the Agreement.

3. Processing of Personal Data.

3.1. **Customer Instructions**.

(a) Obsidian will Process Customer Personal Data as a Processor only: (i) in accordance with Customer Instructions, or (ii) to comply with Obsidian's obligations under applicable laws, subject to any notice requirements under Data Protection Laws.

(b) "**Customer Instructions**" means: (i) Processing to provide the Obsidian Technology and as described in the Agreement (including this DPA) and (ii) other reasonable documented instructions of Customer consistent with the terms of the Agreement

(c) Details regarding the Processing of Customer Personal Data by Obsidian are set forth in Schedule 1 (Subject Matter and Details of Processing).

(d) Obsidian will notify Customer if it receives an instruction that Obsidian reasonably determines infringes Data Protection Laws (but Obsidian has no obligation to actively monitor Customer's compliance with Data Protection Laws). In such an instance, Obsidian will be entitled to suspend performance of such instruction, until Customer confirms in writing that such instruction is valid under Data Protection Laws.

3.2. **Confidentiality**.

(a) Obsidian will protect Customer Personal Data in accordance with its confidentiality obligations as set forth in the Agreement.

(b) Obsidian will ensure personnel who Process Customer Personal Data either enter into written confidentiality agreements or are subject to statutory obligations of confidentiality.

3.3. **Compliance with Laws**.

(a) Obsidian and Customer will each comply with Data Protection Laws in their respective Processing of Personal Data.

(b) Customer will comply with Data Protection Laws in its issuing of Customer Instructions to Obsidian. Customer will ensure that it has established all necessary lawful bases under Data Protection Laws to enable Obsidian to lawfully Process Customer Personal Data for the purposes contemplated by the Agreement (including this DPA), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects. Customer is solely responsible for ensuring the accuracy, quality, and legality of Customer Personal Data Processed by Obsidian including the means by which Customer acquired Personal Data.

3.4. **Changes to Laws**. The Parties will work together in good faith to negotiate an amendment to this DPA as either Party reasonably considers necessary to address the requirements of Data Protection Laws from time to time.

4. Subprocessors.

4.1. **Use of Subprocessors.**

(a) Customer generally authorizes Obsidian to engage Subprocessors to Process Customer Personal Data. Customer further agrees that Obsidian may engage its Affiliates as Subprocessors.

(b) Obsidian will: (i) enter into a written agreement with each Subprocessor imposing data Processing and protection obligations substantially the same as those set out in this DPA and (ii) remain liable for compliance with the obligations of this DPA and for any acts or omissions of a Subprocessor that cause Obsidian to breach any of its obligations under this DPA.

4.2. **Subprocessor List**. Obsidian will maintain an up-to-date list of its Subprocessors, including their functions and locations, as specified in the Subprocessor List set forth in Schedule 1.

4.3. **Notice of New Subprocessors**. Obsidian may update the Subprocessor List from time to time. At least 30 days before any new Subprocessor Processes any Personal Data, Obsidian will add such Subprocessor to the Subprocessor List and notify Customer through email or other means.

4.4. **Objection to New Subprocessors**.

(a) If, within 30 days after notice of a new Subprocessor, Customer notifies Obsidian in writing that Customer objects to Obsidian's appointment of such new Subprocessor based on reasonable data protection concerns, the Parties will discuss such concerns in good faith.

(b) If the Parties are unable to reach a mutually agreeable resolution to Customer's objection to a new Subprocessor, Customer, as its sole and exclusive remedy, may terminate the Order for the affected Obsidian Technology for convenience and Obsidian will refund any prepaid, unused fees for the terminated portion of the Subscription Term.

5. Security.

5.1. **Security Measures**. Obsidian will implement and maintain reasonable and appropriate technical and organizational measures, procedures and practices, as appropriate to the nature of the Customer Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Customer Personal Data and protect against Security Incidents, in accordance with Obsidian's Security Measures referenced in the Agreement and as further described in Schedule 2 (Technical and Organizational Measures). Obsidian will regularly monitor its compliance with its Security Measures and Schedule 2 (Technical and Organizational Measures).

5.2. **Incident Notice and Response**.

(a) Obsidian will implement and follow procedures to detect and respond to Security Incidents.

(b) Obsidian will: (i) notify Customer without undue delay and, in any event, not later than the Specified Notice Period, after becoming aware of a Security Incident affecting Customer and (ii) make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within Obsidian's reasonable control.

(c) Upon Customer's request and taking into account the nature of the applicable Processing, Obsidian will assist Customer by providing, when available, information reasonably necessary for Customer to meet its Security Incident notification obligations under Data Protection Laws.

(d) Customer acknowledges that Obsidian's notification of a Security Incident is not an acknowledgement by Obsidian of its fault or liability.

(e) Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

5.3. **Customer Responsibilities.**

(a) Customer is responsible for reviewing the information made available by Obsidian relating to data security and making an independent determination as to whether the Obsidian Technology meets Customer's requirements and legal obligations under Data Protection Laws.

(b) Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

6. Data Protection Impact Assessment.

Upon Customer's request and taking into account the nature of the applicable Processing, to the extent such information is available to Obsidian, Obsidian will assist Customer in fulfilling Customer's obligations under Data Protection Laws to carry out a data protection impact or similar risk assessment related to Customer's use of the Obsidian Technology, including, if required by Data Protection Laws, by assisting Customer in consultations with relevant government authorities.

7. Data Subject Requests.

7.1. **Assisting Customer**. Upon Customer's request and taking into account the nature of the applicable Processing, Obsidian will assist Customer by appropriate technical and organizational measures, insofar as possible, in complying with Customer's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws, provided that Customer cannot reasonably fulfill such requests independently (including through use of the Obsidian Technology).

7.2. **Data Subject Requests**. If Obsidian receives a request from a Data Subject in relation to the Data Subject's Personal Data, Obsidian will notify Customer and advise the Data Subject to submit the request to Customer (but not otherwise communicate with the Data Subject regarding the request except as may be required by Data Protection Laws), and Customer will be responsible for responding to any such request.

8. Data Return or Deletion.

8.1. **During Term**. During the Term, Customer may, through the features of the Obsidian Technology or such other means, access, return to itself or delete Customer Personal Data.

8.2. **Post Termination.**

(a) Following termination or expiration of the Agreement, Obsidian will, in accordance with its obligations under the Agreement, delete all Customer Personal Data from Obsidian's systems.

(b) Deletion will be in accordance with industry-standard secure deletion practices. Obsidian will issue a certificate of deletion upon Customer's request.

(c) Notwithstanding the foregoing, Obsidian may retain Customer Personal Data: (i) as required by Data Protection Laws or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Obsidian will (x) maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to, retained Customer Personal Data and (y) not further Process retained Personal Data except for such purpose(s) and duration specified in such applicable Data Protection Laws.

9. Audits.

9.1. **Obsidian Records Generally**. Obsidian will keep records of its Processing in compliance with Data Protection Laws and, upon Customer's request, make available to Customer any records reasonably necessary to demonstrate compliance with Obsidian's obligations under this DPA and Data Protection Laws.

9.2. **Third-Party Compliance Program**.

(a) Obsidian will describe its third-party audit and certification programs (if any) and make summary copies of its audit reports (each, an "**Audit Report**") available to Customer upon Customer's written request at reasonable intervals (but not more than once annually) (subject to confidentiality obligations).

(b) Customer may share a copy of Audit Reports with relevant government authorities as required upon their request.

(c) Customer agrees that any audit rights granted by Data Protection Laws will be satisfied by Audit Reports and the procedures of Section 9.3 (Customer Audit) below.

9.3. **Customer Audit**. Obsidian will make available all information necessary to demonstrate its compliance with data protection policies and procedures implemented as part of the Obsidian Technology. To this end, upon written request (not more than once annually) Customer may, at its sole cost and expense, verify Obsidian's compliance with its data protection obligations as specified in this exhibit by: (i) submitting a security assessment questionnaire to Obsidian; and (ii) if Customer is not satisfied with Obsidian's responses to the questionnaire, then Customer may conduct an audit in the form of meetings with Obsidian's information security experts on a mutually agreeable date. Such interviews will be conducted with a minimum of disruption to Obsidian's normal business operations and subject to Obsidian's agreement on scope and timing. Customer may perform the verification described above either itself or by a mutually agreed upon third party auditor, provided that Customer or its authorized auditor executes a mutually agreed upon non-disclosure agreement. Customer will be responsible for any actions taken by its authorized auditor. All information disclosed by Obsidian under this Section 9.3 will be deemed Obsidian Confidential Information, and Customer will not disclose any audit report to any third party except as obligated by law, court order or administrative order by a government agency. Obsidian will remediate any mutually agreed, material deficiencies in its technical and organizational measures identified by the audit procedures described in this Section 9.3 within a mutually agreeable timeframe.

10. Cross-Border Transfers/Region-Specific Terms.

10.1. **Cross-Border Data Transfers.**

(a) Obsidian (and its Affiliates) may Process and transfer Customer Personal Data globally as necessary to provide the Obsidian Technology.

(b) If Obsidian engages in a Restricted Transfer, it will comply with Schedule 3 (Cross-Border Transfer Mechanisms).

10.2. **Region-Specific Terms**. To the extent that Obsidian Processes Personal Data protected by Data Protection Laws in one of the regions listed in Schedule 4 (Region-Specific Terms), then the terms specified therein with respect to the applicable jurisdiction(s) will apply in addition to the terms of this DPA.

SCHEDULE 1 – Subject Matter and Details of Processing

A. LIST OF PARTIES

Data exporter(s):

Name:	The named "Customer" on the signed or accepted Quotation or Agreement.
Address:	The address associated with the Customer on the signed or accepted Quotation or Agreement.

Contact person's name, position and contact details:	The contact details associated with the Customer on the signed or accepted Quotation or Agreement.
Activities relevant to the data transferred under these Clauses:	See Description of Transfer below.
Signature and date:	Refer to the signed or accepted Quotation or Agreement.
Role (controller/processor):	Controller

Data importer(s):

Name:	Obsidian Security, Inc.
Address:	660 Newport Center Drive, Suite 200, Newport Beach, CA, USA 92660
Contact person's name, position and contact details:	The contact details associated with Obsidian on the signed or accepted Quotation or Agreement.
Activities relevant to the data transferred under these Clauses:	See Description of Transfer below.
Signature and date:	Refer to the signed or accepted Quotation or Agreement.
Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred	Individual employee and contractor users of the SaaS applications that Controller has authorized Processor's technology to connect to and individuals whose data are found in the monitored data drawn from Controller's SaaS applications.

Categories of personal data transferred	• Personal identifiers such as given (first, middle) and family (last) names; • Identification numbers such as user-agent strings and identification numbers that may be granted by SaaS applications; • Location data, such as IP addresses and their resolved geographical locations; • Online identifiers such as IP addresses, email addresses, user-agent strings, usernames, and similar online identifiers; and • Incidental data provided by end users through their use of SaaS applications monitored by Processor.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	N/A
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	Ongoing as determined by the Controller.
Nature of the processing	For the provision of the Obsidian Technology and support under the Agreement. Processing activities include: • removing duplicative data; • record linking to combine information about a users' status and activity across all of the SaaS applications that the Customer has granted Obsidian permission to monitor, • identifying accounts with high-risk activity patterns and/or configuration settings, • producing security alerts triggered by anomalous behavior or risky account states, • resolving IP addresses to geographical locations.
Purpose(s) of the data transfer and further processing.	For purposes of providing the Obsidian Technology and support set out in the Agreement and any applicable statement of work.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.	During the Term and as set forth in the Agreement and data retention policies as published in the Documentation.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.	During the Term and as specified under the Agreement.

C. SUBPROCESSORS

The Controller has authorised the use of the following Subprocessors:

The Subprocessors located on the agreed list available on the Trust Portal. As of the effective date, the current list of Subprocessors is:

1. Name: Amazon Web Services
   Address: United States / Germany
   Contact person's name, position and contact details: N/A
   Description of Processing (including a clear delimitation of responsibilities in case several Subprocessors are authorised): Data hosting services for the Obsidian Platform

2. Name: Digital Element
   Address: United States
   Contact person's name, position and contact details: N/A
   Description of Processing (including a clear delimitation of responsibilities in case several Subprocessors are authorised): IP-geolocation provider for the Obsidian Technology.

3. Name: LaunchDarkly
   Address: United States
   Contact person's name, position and contact details: N/A
   Description of Processing (including a clear delimitation of responsibilities in case several Subprocessors are authorised): Product feature enablement.

4. Name: Pendo
   Address: United States
   Contact person's name, position and contact details: N/A
   Description of Processing (including a clear delimitation of responsibilities in case several Subprocessors are authorised): Data analytics platform that generates log data from customer activity.

5. Name: Google
   Address: United States
   Contact person's name, position and contact details: N/A
   Description of Processing (including a clear delimitation of responsibilities in case several Subprocessors are authorised): Data hosting services for the Obsidian Platform and data visualization services.

6. Name: Databricks
   Address: United States
   Contact person's name, position and contact details: N/A
   Description of Processing (including a clear delimitation of responsibilities in case several Subprocessors are authorised): Data platform cloud services provider.

7. Name: Snowflake
   Address: United States
   Contact person's name, position and contact details: N/A
   Description of Processing (including a clear delimitation of responsibilities in case several Subprocessors are authorised): Data warehouse services.

8. Name: Twilio
   Address: United States
   Contact person's name, position and contact details: N/A
   Description of Processing (including a clear delimitation of responsibilities in case several Subprocessors are authorised): Product data enrichment and phone number validation for threat detection; integration with the Obsidian Platform to send tenant registration emails, new product user emails and product notifications.

9. Name: Zendesk
   Address: United States
   Contact person's name, position and contact details: N/A
   Description of Processing (including a clear delimitation of responsibilities in case several Subprocessors are authorised): Customer support platform.

SCHEDULE 2 – Technical and Organizational Measures

Obsidian has taken and will maintain the appropriate administrative, technical, physical and procedural security measures, for the protection of the Customer Personal Data, including the measures set forth below or otherwise made reasonably available by Obsidian. Further Obsidian Technology specific technical and organizational measures will be as set out in the Trust Portal.

Service Security

- **Obsidian Architecture**. Obsidian's Services are designed with multiple layers of protection, covering data transfer, encryption, and network configuration. End users of Obsidian's service can access the Service at any time from web, mobile, and API clients. All of these clients connect to secure services to provide access to the data.

- **Reliability**. Obsidian's Services are developed with redundancies in mission critical architectures to protect against data loss and maintain uptime.

- **Encryption**. To protect Customer Data in transit between the Customer and Obsidian, Obsidian uses TLS 1.3 (256-bit keys) at the browser level and to encrypt the API. Data at rest is protected by 256-bit AES encryption in Amazon Web Services (AWS) S3 buckets and attached EBS volumes. Obsidian's key management infrastructure relies on Customer Managed Keys (CMKs). For sake of clarity and to avoid confusion, Customer Managed Keys is an acronym utilized by AWS and refers here to Obsidian as the customer authorized to manage the Customer Managed Keys.

- **User Management Features**. Obsidian's Platform requires the use of multi-factor authentication.

- **Data Centers**. Obsidian's corporate and production systems are housed at third-party cloud hosted data centers located in the United States and Germany.

Information Security

- **Policies**. Obsidian has established a thorough set of security policies covering areas of information security, physical security, incident response, physical production access, change management and support. These policies are reviewed and approved at least annually. Personnel at Obsidian are notified of updates to these policies and are provided ongoing security and privacy training.

- **Personnel Policy and Access**. Obsidian's internal policies require onboarding procedures that include criminal background checks (as allowed by local laws), educational credential verification, security policy acknowledgement, and non-disclosure agreements. Access reviews are conducted quarterly. Upon termination from Obsidian, personnel access is promptly removed from all Obsidian systems and SaaS accounts. Obsidian employs technical access controls and internal policies to prohibit employees or contractors from arbitrarily accessing Customer data. In order to protect end user privacy and security, only authorized employees and contractors have access to the environment where Customer Data is stored. A record of access request, justification and approval are recorded by management and access is granted to appropriate individuals.

- **Network Security**. Obsidian maintains network security and monitoring techniques that are designed to provide multiple layers of protection and defense. Obsidian employs industry-standard protection techniques, including firewalls, network security monitoring, and intrusion detection systems to ensure only eligible traffic is able to reach Data Importer's infrastructure.

- **Change Management**. Obsidian ensures that security-related changes have been authorized prior to implementation into the production environment. Changes to Obsidian's infrastructure may be made by authorized personnel only.

- **Compliance**. Obsidian undergoes SOC 2 Type 2, ISO 27001, and ISO 27701 security and privacy audits annually. Audits are performed by an independent third party as well as an annual independently conducted penetration test. Obsidian also reviews SOC 1 and/or SOC 2 reports for all subservice organizations. In the event a subservice organization's SOC 1 and/or SOC 2 report is unavailable, Obsidian performs security risk assessments to verify applicable operational security controls and to satisfy control criteria and contractual requirements.

Physical Security

- **Infrastructure**. Physical access to server facilities where production systems reside are controlled by Obsidian's web services providers.

- **Office**. Obsidian maintains access control mechanisms that restrict access to Obsidian facilities. Only employees, contractors, and authorized guests are allowed physical access to Obsidian's office. Authorized guests are escorted while inside the secured perimeter.

SCHEDULE 3 – Cross-Border Transfer Mechanism

1. **Definitions**. Capitalized terms not defined in this Schedule are defined in the DPA.

   1.1. "**EU Standard Contractual Clauses**" or "**EU SCCs**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

   1.2. "**UK International Data Transfer Agreement**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force as of March 21, 2022.

   1.3. In addition:

"**Designated EU Governing Law**" means:	The laws of the Republic of Ireland
"**Designated EU Member State**" means:	Republic of Ireland

2. **EU Transfers**. Where Customer Personal Data is protected by EU GDPR and is subject to a Restricted Transfer, the following applies:

   2.1. The EU SCCs are hereby incorporated by reference as follows:

      (a) Module 2 (Controller to Processor) applies where Customer is a Controller of Personal Data and Obsidian is a Processor of Personal Data;

      (b) Module 3 (Processor to Processor) applies where Customer is a Processor of Personal Data (on behalf of a third-party Controller) and Obsidian is a Processor of Personal Data;

      (c) Customer is the "data exporter" and Obsidian is the "data importer"; and

      (d) by entering into this DPA, each party is deemed to have signed the EU SCCs (including their Annexes) as of the DPA Effective Date.

   2.2. For each Module, where applicable the following applies:

Section Reference	**Clause Application**
Section I, Clause 7	The docking clause does not apply.
Section II, Clause 9	Option 2 will apply, the minimum time period for prior notice of Subprocessor changes shall be as set out in Section 4.3 of this DPA, and Provider shall fulfill its notification obligations by notifying Customer of any Subprocessor changes in accordance with Section 4.3 of this DPA.
Section II, Clause 11	The optional language does not apply.

Section II, Clause 13	All square brackets are removed with the text remaining.
Section IV, Clause 17	Option 1 will apply, and the EU SCCs will be governed by the Designated EU Governing Law.
Section IV, Clause 18 (b)	Disputes will be resolved before the courts of the Designated EU Member State.
Schedule 1 (Subject Matter and Details of Processing)	Contains the information required in Annex 1 of the EU SCCs.
Schedule 2 (Technical and Organisational Measures)	Contains the information required in Annex 2 of the EU SCCs.

2.3. Where context permits and requires, any reference in this DPA to the EU SCCs shall be read as a reference to the EU SCCs as modified in the manner set forth in this Section 2.

3. **Swiss Transfers**. Where Customer Personal Data is protected by the FADP and is subject to a Restricted Transfer, the following applies:

3.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:

Section Reference	**Clause Application**
Section II, Clause 13	The competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner.
Section IV, Clause 17 (Option 1)	The EU SCCs will be governed by the laws of Switzerland.
Section IV, Clause 18 (b)	Disputes will be resolved before the courts of Switzerland.
Section IV, Clause 18 (c)	The term Member State must not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c).
EU GDPR	All references to the EU GDPR in this DPA are also deemed to refer to the FADP.

4. **UK Transfers**. Where Customer Personal Data is protected by the UK GDPR and is subject to a Restricted Transfer, the following applies:

4.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:

(a) each party shall be deemed to have signed the "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under section 119 (A) of the Data Protection Act 2018;

(b) the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of Personal Data;

(c) in Table 1 of the UK Addendum, the parties' key contact information is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(d) in Table 2 of the UK Addendum, information about the version of the EU SCCs, modules and selected clauses which this UK Addendum is appended to are located above in this Schedule 3;

(e) in Table 3 of the UK Addendum:

(i) the list of parties is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;
(ii) the description of transfer is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;
(iii) Annex II is located in Schedule 2 (Technical and Organizational Measures) to this DPA; and
(iv) the list of Subprocessors is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA.

(f) in Table 4 of the UK Addendum, both the Importer and the Exporter may end the UK Addendum in accordance with its terms (and the respective box for each is deemed checked); and

(g) in Part 2: Part 2 - Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with section 119 (A) of the Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of those Mandatory Clauses.

SCHEDULE 4: Region-Specific Terms

A. CALIFORNIA

1. **Definitions**. CCPA/CPRA and other capitalized terms not defined in this Schedule are defined in the DPA.

1.1. "business purpose", "commercial purpose", "personal information", "sell", "service provider" and "share" have the meanings given in the CCPA/CPRA.

1.2. The definition of "Data Subject" includes "consumer" as defined under the CCPA/CPRA.

1.3. The definition of "Controller" includes "business" as defined under the CCPA/CPRA.

1.4. The definition of "Processor" includes "service provider" as defined under the CCPA/CPRA.

2. **Obligations**.

2.1. Customer is providing the Customer Personal Data to Obsidian, acting as a service provider, under the Agreement for the limited and specific business purposes of providing the Obsidian Technology as described in Schedule 1 (Subject Matter and Details of Processing) to this DPA, and otherwise performing under the Agreement.

2.2. Obsidian will comply with its applicable obligations under the CCPA/CPRA and provide the same level of privacy protection to Customer Personal Data as is required by the CCPA/CPRA.

2.3. Obsidian acknowledges that Customer has the right to: (i) take reasonable and appropriate steps under Section 9 (Audits) of this DPA to help to ensure that Obsidian use of Customer Personal Data is consistent with Customer's obligations under the CCPA/CPRA, (ii) receive from Obsidian notice and assistance under Section 7 (Data Subject Requests) of this DPA regarding consumers' requests to exercise rights under the CCPA/CPRA and (iii) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data.

2.4. Obsidian will notify Customer promptly after it makes a determination that it can no longer meet its obligations under the CCPA/CPRA.

2.5. Absent Customer Instructions or the Customer's prior written agreement, or generating Aggregate Data or Anonymous Data, Obsidian will not retain, use or disclose Customer Personal Data: (i) for any purpose,

including a commercial purpose, other than the business purposes described in Section 2.1 of this Section A (California) of Schedule 4, or (ii) outside of the direct business relationship between Obsidian with Customer, except, in either case, where and to the extent permitted by the CCPA/CPRA.

2.6. Obsidian will not sell or share Customer Personal Data received under the Agreement.

2.7. Obsidian will not combine Customer Personal Data with other personal information except to the extent a service provider is permitted to do so by the CCPA/CPRA.

Last Updated: February 6, 2025