**OBSIDIAN SECURITY, INC.**

**SUPPLIER DATA PROCESSING ADDENDUM**

This Data Processing Addendum, including its Annexes and the Standard Contractual Clauses (the "**DPA**"), is incorporated by reference into each agreement between Obsidian Security, Inc. or its Affiliate ("**Obsidian**") and the entity that has entered into such agreement as a service provider, vendor, or contractor ("**Vendor**") (each such agreement, the "**Agreement**") and applies solely to the extent that Vendor processes any Obsidian Personal Data (defined below) in connection with the Services. By entering into an Agreement that references this DPA, Vendor agrees to be bound by the terms herein. Obsidian enters into this DPA on behalf of itself and, if applicable and to the extent required under Applicable Data Protection Laws, in the name and on behalf of its Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

**1. Definitions.**

1.1. "**Affiliate**" means any entity (a) that the party Controls; (b) that the party is Controlled by; or (c) with which the party is under common Control, where "Control" means direct or indirect control (including by ownership) of fifty percent (50%) of an entity's voting interests.

1.2. "**Applicable Data Protection Laws**" means all data protection and privacy laws and regulations applicable to the respective party in its role in the processing of Obsidian Personal Data under the Agreement, which may include, to the extent applicable, European Data Protection Laws, the Personal Information Protection and Electronic Documents Act, the CCPA, the Colorado Privacy Act, the Connecticut Personal Data Privacy and Online Monitoring Act, the Virginia Consumer Data Privacy Act, and the Utah Consumer Privacy Act.

1.3. "**CCPA**" means the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 ("CPRA") (Cal. Civ. Code §§ 1798.100 et seq.), as may be amended, superseded, or replaced from time to time.

1.4. "**Obsidian Personal Data**" means any "**personal data**" or "**personal information**" that Obsidian provides to Vendor or that Vendor processes on behalf of Obsidian in connection with the Services. For the avoidance of doubt, this includes the “personal data” of Obsidian’s customers which Obsidian processes.

1.5. "**Data Privacy Framework**" means the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs (as applicable) operated by the U.S. Department of Commerce, as may be amended, superseded or replaced.

1.6. "**Documentation**" means documentation provided by Vendor that describes the performance, features, functionality, administrative, physical, and technical measures in place for protection of the security and integrity of the Services (the "Security Policies").

1.7. "**European Data Protection Laws**" means (a) Regulation 2016/679 (General Data Protection Regulation) ("EU GDPR"); (b) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"); and (c) the Swiss Federal Data Protection Act and its implementing regulations ("Swiss Data Protection Act"); in each case as may be amended, superseded or replaced from time to time.

1.8. "**Restricted Transfer**" means a transfer (directly or via onward transfer) of personal data that is subject to European Data Protection Laws to a third country outside the European Economic Area, United Kingdom, and Switzerland which is not subject to an adequacy determination by the European Commission, United Kingdom, or Swiss authorities (as applicable).

1.9. "**Security Breach**" means a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Obsidian Personal Data.

1.10. "**Services**" means the services, software, or other deliverables provided by Vendor to Obsidian under the Agreement.

1.11. "**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021, as may be amended, superseded, or replaced from time to time.

1.12. "**Subprocessor**" means any other processor engaged by Vendor to process Obsidian Personal Data.

1.13. "**UK Addendum**" means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioner's Office under S.119(a) of the UK Data Protection Act 2018, as updated or amended from time to time.

1.14. The terms "**controller**", "**data subject**", "**supervisory authority**", "**processor**", "**process**", "**processing**", "**personal data**", and "**personal information**" shall have the meanings given to them in Applicable Data Protection Laws. The term "**controller**" includes "**business**", the term "**data subject**" includes "**consumers**", and the term "**processor**" includes "**service provider**" (in each case, as defined by the CCPA).

**2. Processing of Personal Data.**

2.1. **Scope and Roles of the Parties.** This DPA applies when Obsidian Personal Data is processed by Vendor as a processor in its provision of the Services to Obsidian, who will act as either a controller or processor of Obsidian Personal Data, as applicable.

2.2. **Obsidian Processing.** Obsidian agrees that it will comply with its obligations under Applicable Data Protection Laws in its processing of Obsidian Personal Data and any processing instructions it issues to Vendor.

2.3. **Vendor Processing.** Vendor agrees that when Vendor processes Obsidian Personal Data in its capacity as a processor on behalf of Obsidian, Vendor will (a) comply with Applicable Data Protection Laws; and (b) process Obsidian Personal Data as necessary to perform its obligations under the Agreement, and only in accordance with Obsidian's documented instructions (as set forth in the Agreement, in this DPA, or as otherwise directed by Obsidian in writing). Vendor is not responsible for determining if Obsidian's processing instructions are compliant with applicable law. However, Vendor shall notify Obsidian in writing if, in its reasonable opinion, Obsidian's processing instructions infringe Applicable Data Protection Laws.

2.4. **Details of Processing.** The details of the processing of Obsidian Personal Data by Vendor are set out in Annex A to the DPA.

3. **Confidentiality.** Vendor shall ensure that any employees or personnel it authorizes to process Obsidian Personal Data are subject to an appropriate duty of confidentiality.

4. **Subprocessing.**

4.1. **Authorization**. Obsidian provides a general authorization to Vendor's use of Subprocessors to process Obsidian Personal Data in accordance with this Section, including those Subprocessors identified in Vendor's subprocessor list provided to Obsidian (the "Subprocessor List"). Vendor shall provide its current Subprocessor List to Obsidian upon request, and the template for such list is set forth in Annex C.

4.2. **Subprocessor Obligations.** Vendor shall (a) enter into a written agreement with its Subprocessors that includes data protection and security measures no less protective than the measures set forth in this DPA; and (b) remain fully liable for any breach of the Agreement and this DPA that is caused by an act, error, or omission of its Subprocessors to the extent that Vendor would have been liable for such act, error, or omission had it been caused by Vendor.

4.3. **Subprocessor Changes.** At least sixty (60) calendar days prior to the date on which any new Subprocessor shall commence processing Obsidian Personal Data, Vendor shall update the Subprocessor List and notify Obsidian of such update in writing.

4.4. **Subprocessor Objections.** Obsidian may object to Vendor's appointment of a new Subprocessor on reasonable grounds relating to data protection by notifying Vendor in writing within thirty (30) calendar days after Vendor's notification pursuant to Section 4.3. In such an event, Vendor and Obsidian will discuss those objections in good faith with a view to achieving resolution. If the parties are not able to achieve resolution within ten (10) calendar days from Obsidian's written notification, Obsidian may terminate the portion of the Agreement with respect to those Services that cannot be provided by Vendor without the use of the new Subprocessor. Vendor will provide Obsidian with a pro rata reimbursement of any prepaid, but unused fees following the effective date of such termination.

5. **Assistance.**

5.1. **Data Subject Access Requests.** Obsidian is responsible for responding to and complying with data subject requests ("DSAR"). Upon request from Obsidian, Vendor shall, taking into account the nature of the processing, reasonably cooperate with Obsidian to enable Obsidian to respond to the DSAR. If a data subject sends a DSAR to Vendor directly and where Obsidian is identified or identifiable from the request, Vendor will promptly forward such DSAR to Obsidian and Vendor shall not, unless legally compelled to do so, respond directly to the data subject except to refer them to Obsidian to allow Obsidian to respond as appropriate. If Obsidian is not identified or identifiable, Vendor will notify the data subject that it is a processor and to contact the relevant controller and will not otherwise respond.

5.2. **Data Protection Impact Assessments.** Vendor will provide reasonably requested information regarding the Services to Obsidian to carry out data protection impact assessments relating to the processing of Obsidian Personal Data and any related required consultation with supervisory authorities as required by Applicable Data Protection Laws, so long as Obsidian does not otherwise have access to the relevant information.

5.3. **Legal Requests.** If Vendor receives a subpoena, court order, warrant, or other legal demand from law enforcement or any public or judicial authority seeking the disclosure of Obsidian Personal Data, Vendor will attempt to redirect the governmental body to request such

Obsidian Personal Data directly from Obsidian. As part of this effort, Vendor may provide Obsidian's basic contact information to the governmental body. If compelled to disclose Obsidian Personal Data to a governmental body, Vendor will give Obsidian reasonable notice of the legal demand to allow Obsidian to seek a protective order or other appropriate remedy, unless Vendor is legally prohibited from doing so.

**6. Security.**

6.1. **Security Measures.** As set forth in the Documentation and provided in the Agreement, Vendor has implemented the Security Policies. The Security Policies are subject to technical progress and development, and Vendor may update the Security Policies, provided that any updates shall not materially diminish the overall security of Obsidian Personal Data or the Services.

6.2. **Security Breach Notification.** In the event of a Security Breach, Vendor will (a) notify Obsidian in writing without undue delay and in no event later than seventy-two (72) hours after becoming aware of the Security Breach; and (b) promptly take reasonable steps to contain, investigate, and mitigate any adverse effects resulting from the Security Breach. Vendor will reasonably cooperate with and assist Obsidian with respect to any required notification to supervisory authorities or data subjects (as applicable), taking into account the nature of the processing, the information available to Vendor, and any restrictions on disclosing the information (such as confidentiality).

**7. Audits and Records.**

7.1. **Audit Program.** Upon written request and at no additional cost to Obsidian, Vendor shall provide Obsidian, and/or its appropriately qualified third-party representative, access to reasonably requested documentation evidencing Vendor's compliance with its obligations under this DPA in the form of the relevant audits or certifications listed in the Security Policies. Such audits shall be performed at least once annually by independent third-party security professionals selected by Vendor. Such audits result in the generation of a confidential audit report ("Audit Report").

7.2. **Obsidian Audit.** Obsidian may send a written request to conduct an audit of Vendor's applicable controls on an annual basis (an "Obsidian Audit"). Vendor and Obsidian shall mutually agree on the details of the audit, including the reasonable start date, scope and duration of, and security and confidentiality controls applicable to any such Obsidian Audit. Obsidian shall bear the costs of such Obsidian Audit unless the audit reveals a material breach of this DPA by Vendor.

7.3. **Confidentiality of Audit Reports.** The Audit Reports, the results of any Obsidian Audit, and any information arising therefrom shall be considered Vendor Confidential Information and may only be shared with a third party with Vendor's prior written agreement, except that Obsidian may share such information with its customers to the extent required to satisfy Obsidian's obligations to such customers under Applicable Data Protection Laws.

**8. Transfer of Personal Data.**

8.1. **Restricted Transfers.** Where the transfer of Obsidian Personal Data to Vendor is a Restricted Transfer, such transfer shall be governed by (a) the Data Privacy Framework so long as the Data Privacy Framework has not been invalidated and Vendor remains certified; or (b) the Standard Contractual Clauses, which shall be deemed incorporated into and form an integral part of the Agreement in accordance with Annex B of this DPA.

8.2. **Alternative Transfer Mechanisms.** If and to the extent that a court of competent jurisdiction or a supervisory authority with binding authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer Obsidian Personal Data to Vendor, the parties shall reasonably cooperate to agree and take any actions that may be reasonably required to implement any additional measures or alternative transfer mechanism to enable the lawful transfer of such Obsidian Personal Data. Such alternative transfer mechanism shall apply instead of the SCCs described in Section 8.1 of this DPA (but only to the extent such alternative transfer mechanism complies with applicable European Data Protection Laws and extends to the territories to which Obsidian Personal Data is transferred).

**9. Deletion and Return.** Upon termination or expiration of the Agreement and following Obsidian's written request, Vendor will delete or return (at Obsidian's election) any Obsidian Personal Data within its possession or control within thirty (30) days following such request. Upon Obsidian's request, Vendor shall certify in writing that it has complied with its obligations under this Section.

**10. CCPA Compliance.** Vendor shall not process, retain, use, or disclose Obsidian Personal Data for any purpose other than for the purposes set out in the Agreement and this DPA and as permitted under the CCPA. Vendor shall not sell or share Obsidian Personal Data, as those terms are defined under the CCPA. Vendor shall not combine Obsidian Personal Data with personal information that Vendor receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, unless expressly permitted under the CCPA.

**11. General.**

11.1. The parties agree that this DPA shall replace any existing data processing addendum, attachment, exhibit, or standard contractual clauses that the parties may have previously entered into in connection with the Services. Obsidian may update this DPA from time to time by posting a revised version at the URL where this DPA is made available; provided that any such update shall not materially diminish the protections afforded to Obsidian Personal Data. If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

11.2. In the event of any conflict between this DPA and any data privacy provisions set out in any agreements between the parties relating to the Services, the parties agree that the terms of this DPA shall prevail, provided that if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses control and take precedence.

11.3. This DPA will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Laws.

11.4. The obligations placed upon each party under this DPA and the Standard Contractual Clauses shall survive so long as Vendor processes Obsidian Personal Data on behalf of Obsidian.

This DPA is effective as of the effective date of the applicable Agreement and does not require a separate signature.

## ANNEX A

## DESCRIPTION OF THE PROCESSING / TRANSFER

**ANNEX 1(A): LIST OF PARTIES**

**Data exporter**

| | |
|---|---|
| **Name:** | Obsidian Security, Inc. or the Obsidian Affiliate identified in the applicable Agreement or Statement of Work. |
| **Contact person's name, position, and contact details:** | As specified in the Agreement or as otherwise provided to Vendor. |
| **Activities relevant to the data transferred:** | The activities specified in Annex 1(B) below. |
| **Signature and date:** | By entering into an Agreement that references this DPA. |
| **Role:** | Controller (for Module 2) or Processor (for Module 3). |

**Data importer**

| | |
|---|---|
| **Name:** | The entity identified as "Vendor" in the Agreement and this DPA. |
| **Contact person's name, position, and contact details:** | As specified in the Agreement or as otherwise provided to Obsidian. |
| **Activities relevant to the data transferred:** | The activities specified in Annex 1(B) below. |
| **Signature and date:** | By entering into an Agreement that references this DPA. |
| **Role:** | Processor or Subprocessor |

**ANNEX 1(B): DESCRIPTION OF THE PROCESSING / TRANSFER**

| | |
|---|---|
| **Categories of data subjects whose personal data is transferred:** | Individual employee and contractor users of Obsidian's Services and the associated information gathered by the SaaS applications that Obsidian's customers have authorized Obsidian's technology to connect to and individuals whose data are found in the monitored data drawn from Obsidian's customer's monitored 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;<br>● Location data, such as IP addresses and their resolved geographical locations;<br>● Online identifiers such as IP addresses, email addresses, user-agent strings, usernames, and similar online identifiers; and<br>● Incidental data provided by end users through their use of SaaS applications monitored by Processor. |
| **Sensitive data transferred (if appropriate):** | N/A |
| **Frequency of the transfer:** | Continuous |
| **Nature, subject matter, and duration of the processing:** | For the provision of the Services and support under the Agreement |
| **Purpose(s) of the data transfer and further processing:** | Providing the Services and support set out in the Agreement. |
| **Period for which the personal data will be retained:** | For the duration of the Agreement, unless otherwise specified in the Agreement or required by applicable law. |
| **For transfers to (sub-)processors, also specify subject matter, nature, and duration of the processing:** | As specified by Vendor in the Subprocessor List. |

**ANNEX 1(C): COMPETENT SUPERVISORY AUTHORITY**

| | |
|---|---|
| **Competent supervisory authority:** | The data exporter's competent supervisory authority will be determined in accordance with the EU GDPR. |

**ANNEX B**

**STANDARD CONTRACTUAL CLAUSES (Modules 2 and 3)**

1. Subject to Section 8.1 of the DPA, where the transfer of Obsidian Personal Data to Vendor is a Restricted Transfer and Applicable Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be governed by the Standard Contractual Clauses, which shall be deemed incorporated into and form part of the DPA as follows:

    a. In relation to transfers of Obsidian Personal Data protected by the EU GDPR, the SCCs shall apply as follows:

        i. Module Two terms shall apply (where Obsidian is the controller of Obsidian Personal Data) and Module Three terms shall apply (where Obsidian is a processor of Obsidian Personal Data on behalf of its customers);

        ii. in Clause 7, the optional docking clause shall apply and Obsidian Affiliates may accede to the SCCs under the same terms and conditions as Obsidian, subject to mutual agreement of the parties;

        iii. in Clause 9, Option 2 ("general authorization") is selected, and the process and time period for prior notice of Subprocessor changes shall be as set out in Section 4.3 of the DPA;

        iv. in Clause 11, the optional language shall not apply;

        v. in Clause 17, Option 1 shall apply and the SCCs shall be governed by Irish law;

        vi. in Clause 18(b), disputes shall be resolved before the courts of Ireland;

        vii. Annex I shall be deemed completed with the information set out in Annex A to the DPA; andviii. Annex II shall be deemed completed with the information set out in the Security Policies, subject to Section 6.1 (Security Measures) of the DPA.

    b. In relation to transfers of Obsidian Personal Data protected by the UK GDPR, the SCCs as implemented under Section 1(a) above shall apply with the following modifications:

        i. the SCCs shall be modified and interpreted in accordance with Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of the DPA;

        ii. Tables 1, 2, and 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in Annex A and Annex B to the DPA and the Security Policies respectively, and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party"; and

        iii. any conflict between the terms of the SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

    c. In relation to transfers of Obsidian Personal Data protected by the Swiss Data Protection Act, the SCCs as implemented under Section 1(a) above will apply with the following modifications:

        i. references to "Regulation (EU) 2016/679" and specific articles therein shall be interpreted as references to the Swiss Data Protection Act and the equivalent articles or sections therein;

        ii. references to "EU", "Union", "Member State", and "Member State law" shall be replaced with references to "Switzerland" and/or "Swiss law" (as applicable);

iii. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection and Information Commissioner" and "applicable courts of Switzerland";

iv. the SCCs shall be governed by the laws of Switzerland; andv. disputes shall be resolved before the competent Swiss courts.

2. Where the Standard Contractual Clauses apply pursuant to Section 8.1 of this DPA, this section sets out the parties' interpretations of their respective obligations under specific provisions of the Clauses, as identified below. Where a party complies with the interpretations set out below, that party shall be deemed by the other party to have complied with its commitments under the Standard Contractual Clauses:

   a. where Obsidian is itself a processor of Obsidian Personal Data acting on behalf of a third-party controller and Vendor would otherwise be required to interact directly with such third-party controller (including notifying or obtaining authorizations from such third-party controller), Vendor may interact solely with Obsidian and Obsidian shall be responsible for forwarding any necessary notifications to and obtaining any necessary authorizations from such third-party controller;

   b. the certification of deletion described in Clause 16(d) of the SCCs shall be provided by Vendor to Obsidian upon Obsidian's written request;

   c. for the purposes of Clause 15(1)(a) of the SCCs, Vendor shall notify Obsidian and not the relevant data subject(s) in case of government access requests, and Obsidian shall be solely responsible for notifying the relevant data subjects as necessary; and

   d. taking into account the nature of the processing, Obsidian agrees that it is unlikely that Vendor would become aware that Obsidian Personal Data processed by Vendor is inaccurate or outdated. To the extent Vendor becomes aware of such inaccurate or outdated data, Vendor will inform Obsidian in accordance with Clause 8.4 of the SCCs.

## ANNEX C

### Subprocessor List

| Sub-processor Legal Name | Address/Location of Processing | Description of the Services and/or Purposes for the Sub-processing | Contact Information |
|---|---|---|---|
| | | | |
| | | | |
| | | | |