OBSIDIAN SECURITY, INC.

DATA PROCESSING ADDENDUM

1. Scope. This Data Processing Agreement ("**DPA**"), including its Annexes and the Standard Contractual Clauses, applies solely to the extent that Obsidian processes Subscriber Personal Data (defined below) in connection with the Services. The DPA applies for the duration of Obsidian's processing of Subscriber Personal Data. By entering into the Agreement, Subscriber enters into this DPA on behalf of itself and, to the extent required under Applicable Data Protection Laws, on behalf of its Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. Except where otherwise indicated, the term "**Subscriber**" shall include Subscriber and its Authorized Affiliates.

2. Definitions.

2.1. **"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 Subscriber 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, the Utah Consumer Privacy Act and any other applicable data protection or privacy law.

2.2. **"Authorized Affiliate**" means a Subscriber Affiliate who is authorized to use the Services under the Agreement and who has not signed their own separate agreement with Obsidian.

2.3. **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq*., as amended by the California Privacy Rights Act, and its implementing regulations.

2.4. "**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Framework self-certification programs (as applicable) operated by the U.S. Department of Commerce; as may be amended, superseded or replaced.

2.5. **"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Data Protection Act and its implementing regulations ("**Swiss Data Protection Act**"); in each case as may be amended, superseded or replaced from time to time.

2.6. **"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).

2.7. **"Security Breach"** means an actual or reasonably suspected breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Subscriber Personal Data.

2.8. **"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.

2.9. **"Subscriber Personal Data"** means any "personal data" or "personal information" contained within Subscriber Data that is processed by the Services.

2.10. **"Subprocessor"** means any other processor engaged by Obsidian to process Subscriber Personal Data.

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

2.12. 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).

3. Processing of Personal Data

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

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

3.3. **Obsidian Processing.** Obsidian agrees that (a) when Obsidian processes Subscriber Personal Data in its capacity as a processor on behalf of the Subscriber, Obsidian will (i) comply with Applicable Data Protection Laws, and (ii) process the Subscriber Personal Data as necessary to perform its obligations under the Agreement, and only in accordance with Subscriber's documented instructions (as set forth in the Agreement, in this DPA, or as directed by the Subscriber or Subscriber's Authorized Users through the Services). Obsidian is not responsible for determining if Subscriber's processing instructions are compliant with applicable law. However, Obsidian shall notify Subscriber in writing if, in its reasonable opinion, the Subscriber's processing instructions infringe Applicable Data Protection Laws and provided that Subscriber acknowledges that Subscriber Personal Data may be processed on an automated basis in accordance with Subscribers' use of the Services, which Obsidian does not monitor.

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

4. Confidentiality. Obsidian shall ensure that any employees or personnel it authorizes to process Subscriber Personal Data is subject to an appropriate duty of confidentiality.

5. Subprocessing

5.1. **Authorization.** Subscriber provides a general authorization to Obsidian's use of Subprocessors to process Subscriber Personal Data in accordance with this Section, including those Subprocessors listed in the Documentation or in such other location as Obsidian may notify Subscriber from time to time (the "**Subprocessor List**").

5.2. **Subprocessor Obligations.** Obsidian shall (i) enter into a written agreement with its Subprocessors, which includes data protection and security measures no less protective than the measures set forth in this DPA; and (ii) 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 Obsidian would have been liable for such act, error or omission had it been caused by Obsidian.

5.3. **Subprocessor Changes.** At least thirty (30) calendar days prior to the date on which any new Subprocessor shall commence processing Subscriber Personal Data, Obsidian shall update the Subprocessor List and individuals who have signed up to receive updates to the Subprocessor List via the mechanism(s) indicated on the Subprocessor List will be notified of that update.

5.4. **Subprocessor Objections.** Subscriber may object to Obsidian' appointment of a new Subprocessor on reasonable grounds relating to data protection by notifying Obsidian in writing at compliance@Obsidian.com within ten (10) calendar days after Obsidian's update of the Subprocessor List pursuant to Section 5.3. In such an event, Obsidian and Subscriber will discuss those objections in good faith with a view to achieving resolution**.** If the parties are not able to achieve resolution, within thirty (30) calendar days from Subscriber's written notification, Subscriber, as its sole and exclusive remedy, may terminate the Order Form(s) with respect to only those aspects which cannot be provided by Obsidian without the use of the new

Subprocessor. Obsidian will provide Subscriber with a pro rata reimbursement of any prepaid, but unused fees of such Order Form(s) following the effective date of such termination.

6. Assistance

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

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

6.3. **Legal Requests.** If Obsidian receives a subpoena, court order, warrant or other legal demand from law enforcement or any public or judicial authority seeking the disclosure of Subscriber Personal Data, Obsidian will attempt to redirect the governmental body to request such Subscriber Personal Data directly from Subscriber. As part of this effort, Obsidian may provide Subscriber's basic contact information to the governmental body. If compelled to disclose Subscriber Personal Data to a governmental body, Obsidian will give Subscriber reasonable notice of the legal demand to allow Subscriber to seek a protective order or other appropriate remedy, unless Obsidian is legally prohibited from doing so.

7. Security

7.1. **Security Measures.** As set forth in the Documentation and provided in the Agreement, Obsidian has implemented the Security Measures. The Security Measures are subject to technical progress and development and Obsidian may update the Security Measures, provided that any updates shall not materially diminish the overall security of Subscriber Personal Data or the Services. Obsidian may make available certain security controls within the Services that Subscriber may use in accordance with the Documentation.

7.2. **Security Breach Notification.** In the event of a Security Breach, Obsidian will (a) notify Subscriber in writing without undue delay and in no event later than forty-eight (48) 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. Obsidian will reasonably cooperate with and assist Subscriber 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 Obsidian, and any restrictions on disclosing the information (such as confidentiality).

8. Audits and Records

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

8.2. **Audit.** Only to the extent Subscriber cannot reasonably satisfy Obsidian compliance with this DPA through the Audit Reports, or where required by Applicable Data Protection Laws, Subscriber may send a written request to conduct an audit of Obsidian applicable controls on an annual basis. Obsidian and Subscriber 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 audit. The Audit Report, audit, and any information arising therefrom shall be considered Obsidian Confidential Information and may only be shared with a third party (including a third party controller) with Obsidian prior written agreement**.**

9. Transfer of Personal Data

9.1. **Restricted Transfers.** Where the transfer of Subscriber Personal Data to Obsidian is a Restricted Transfer, such transfer shall be governed by (i) the Data Privacy Framework so long as the Data Privacy Framework has not been invalidated and Obsidian is certified; or (ii) 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.

9.2. **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 Subscriber Personal Data to Obsidian, 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 Subscriber Personal Data, such alternative transfer mechanism shall apply instead of the SCCs described in Section 9.1 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 Subscriber Personal Data is transferred).

10. Deletion and Return. Obsidian will assist Subscriber in deleting or retrieving Subscriber Personal Data upon written request in accordance with the functionality of the Services. Upon termination or expiration of the Agreement Obsidian will delete any Subscriber Personal Data within its possession or control within seven (7) days following the effective date of such termination or expiration, unless a different period is specified in the applicable Order Form.

11. CCPA Compliance. Obsidian shall not process, retain, use, or disclose Subscriber Personal Data for any purpose other than for the purposes set out in the Agreement, DPA and as permitted under the CCPA. Obsidian shall not sell or share information as those terms are defined under the CCPA.

12. General

12.1. This DPA supersedes any prior data processing agreement between the parties. If changes in Applicable Data Protection Laws require amendment of this DPA, the parties shall negotiate in good faith to make the minimum changes necessary to achieve compliance. If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

12.2. Obsidian's obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to the following conditions: (a) Subscriber is solely responsible for communicating any additional processing instructions on behalf of its Authorized Affiliates; (b) Subscriber shall be responsible for Authorized Affiliates' compliance with this DPA and all acts and/or omissions by an Authorized Affiliate with respect to Subscriber's obligations under this DPA; and (c) if an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against Obsidian ("**Authorized Affiliate Claim**"), Subscriber must bring such Authorized Affiliate Claim directly against Obsidian on behalf of such Authorized Affiliate, unless Applicable Data Protection Laws require the Authorized Affiliate be a party to such claim, and all Authorized Affiliate Claims shall be considered claims made by Subscriber and shall be subject to any liability restrictions set forth in the Agreement, including any aggregate limitation of liability. In no event will this DPA or any party restrict or limit the rights of any data subject or of any competent supervisory authority.

12.3. 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.

12.4. 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.

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

ANNEX A

DESCRIPTION OF THE PROCESSING / TRANSFER

ANNEX 1(A): LIST OF PARTIES	
Data exporter	**Name of the data exporter:** The entity identified as the "Subscriber" in the Agreement and this DPA. **Contact person's name, position, and contact details:** The address and contact details associated with Subscriber's Obsidian account, or as otherwise specified in this DPA or the Agreement. **Activities relevant to the data transferred:** The activities specified in Annex 1(B)below. **Signature and date**: By acceptance of the Agreement and its effective date **Role (Controller/Processor):** Controller (for Module 2) or Processor (for Module 3).
Data importer	**Name of the data importer:** Obsidian Security, Inc. or the Obsidian Affiliate named on the applicable Order Form **Contact person's name, position, and contact details:** The person identified in the Documentation for a specific Service **Activities relevant to the data transferred:** The activities specified in Annex 1.B below. **Signature and date**: By acceptance of the Agreement and its effective date **Role (Controller/Processor):** 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 the Third-Party Applications that Subscriber has authorized Obsidian's services to connect to and individuals whose data are found in the monitored data drawn from Subscriber's Third-Party 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 Third-Party 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 Third-Party Applications monitored by Processor.
Sensitive data transferred (if appropriate)	N/A
Frequency of the Transfer	Continuous

Nature, subject matter, and duration of the processing:	• Removing duplicative data; • Record linking to combine information about a users' status and activity across all of the Third-Party 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:	Providing the Services set out in the Agreement and any applicable Order Form or statement of work.
Period for which the personal data will be retained:	Obsidian will retain Subscriber Personal Data for the term of the Agreement and any period after the termination of expiry of the Agreement during which Obsidian processes Subscriber Personal Data in accordance with the Agreement.
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.
Subprocessors	
Subprocessor List	Obsidian's list of subprocessors is available at trust.obsidiansecurity.com

ANNEX B

STANDARD CONTRACTUAL CLAUSES (Modules 2 and 3)

1. Subject to Section 9.1 of the DPA, where the transfer of Subscriber Personal Data to Obsidian 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:

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

a. Module Two terms shall apply (where Subscriber is the controller of Subscriber Personal Data) and the Module Three terms shall apply (where Subscriber is the processor of Subscriber Personal Data);

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

c. in Clause 9, option 2 ("**general authorization**") is selected, and the process and time period for prior notice of Sub-processor changes shall be as set out in Section 5.3 of the DPA;

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

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

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

g. Annex I shall be deemed completed with the information set out in Annex A to the DPA; and

h. Annex II shall be deemed completed with the information set out in the Security Measures, subject to Section 7.1 (Security Measures) of the DPA.

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

a. 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;

b. 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 Measures respectively, and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party"; and

c. 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.

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

a. 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;

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

c. 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");

d. the SCCs shall be governed by the laws of Switzerland; and

e. disputes shall be resolved before the competent Swiss courts.

2. Where the Standard Contractual Clauses apply pursuant to Section 9.1 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:

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

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

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

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