This Data Processing Addendum ("DPA") is incorporated into and forms part of Securonix Master Software as a Service Agreement, or such other agreement by and between Securonix, Inc., a Delaware Corporation, acting on its own behalf and as agent for each Securonix Affiliate ("Securonix"); and (ii) _____, _____, acting on its own behalf and as agent for each Company Affiliate ("Company") ("Principal Agreement") under which Securonix processes data on behalf of Company as part of performing under that agreement ("Services"). This DPA is effective as of the last signature date set forth below ("DPA Effective Date").

1.   Definitions.

1.1   In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1   "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.1.2   "**Contracted Processor**" means Securonix or a Subprocessor;

1.1.3   "**Data Protection Laws**" means any applicable laws governing data protection and security, including the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**"), the United Kingdom Data Protection Act (2018) ("**UK 2018 Privacy Act**"), and the Swiss Federal Data Protection Act ("**FADP**");

1.1.4   "**EU SCCs**" means the Standard Contractual Clauses issued pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 *on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, located http://data.europa.eu/eli/dec_impl/2021/914/oj., and completed as set forth in Section 10 below.

1.1.5   "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Securonix for Company pursuant to the Principal Agreement;

1.2   The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the applicable Data Protection Law.

1.3   The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2.   Processing of Company Personal Data. Annex I.B below sets out certain information regarding Securonix's Processing of the Company Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Company may make reasonable amendments to Annex I.B by written notice to Securonix from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Annex

I.B (including as amended pursuant to this section) confers any right or imposes any obligation on any party to this DPA.

3. Security.

3.1   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, Securonix will, in relation to the Company Personal Data, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR, and in accordance with Annex II herein..

3.2   In assessing the appropriate level of security, Securonix will take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

4. Subprocessing.

4.1   Company authorizes Securonix to appoint (and permit each Subprocessor appointed in accordance with this section 4 to appoint) Subprocessors in accordance with this section 4 and any restrictions in the Principal Agreement.

4.2   Securonix may continue to use those Subprocessors already engaged by Securonix as at the date of this DPA, subject to Securonix in each case as soon as practicable meeting the obligations set out in section 4.4.

4.3   Securonix will give Company prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within ten (10) of receipt of that notice, Company notifies Securonix in writing of any objections (on reasonable grounds) to the proposed appointment, the parties will seek to resolve the matter in good faith. If Securonix can provide the Services to Company without using the Subprocessor and decides in its discretion to do so, then Company will have no further rights to object the Subprocessor under this Section 4.3.

4.4   With respect to each Subprocessor, Securonix or the relevant Securonix Affiliate shall:

4.4.1   before the Subprocessor first Processes Company Personal Data (or, where relevant, in accordance with section 4.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement;

4.4.2   ensure that the arrangement between on the one hand (a) Securonix, or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this DPA and meet the requirements of article 28(3) of the GDPR;

4.4.3   if that arrangement involves a data transfer in accordance with Section 11 below, ensure that the appropriate standard contractual clauses are at all relevant times incorporated into the agreement between on the one hand (a) Securonix, (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Company Personal Data procure that it enters into an agreement incorporating the appropriate standard contractual with the Company; and

4.4.4   provide to Company for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this DPA) as Company may request from time to time.

4.5   Securonix and each Securonix Affiliate shall ensure that each Subprocessor performs the obligations under this DPA as they apply to Processing of Company Personal Data carried out by that Subprocessor, as if it were party to this DPA in place of Securonix.

5.   **Data Subject Rights.** Securonix will provide all reasonable and timely assistance (including by appropriate technical and organizational measures) to Company to enable Company to respond to: (i) any request from a data subject to exercise any of its rights under applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, inquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Securonix, Securonix will promptly inform Company providing full details of the same.

6.   **Data Protection Impact Assessment and Prior Consultation.** Securonix will provide Company with reasonable assistance with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

7.   **Deletion or return of Company Personal Data.** Upon termination or expiration of the Principal Agreement, Securonix will (at Company's election) destroy or return to Company all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a third party for processing). This requirement will not apply to the extent that Securonix is required by any EU (or any EU Member State) law to retain some or all of the Data, in which event Securonix will isolate and protect the Data from any further processing except to the extent required by such law.

8.   **Audit rights.** Securonix will permit Company (or its appointed third-party auditors) to audit Securonix's compliance with this DPA, and will make available to Company all information, systems and staff necessary for Company (or its third-party auditors) to conduct such audit. Securonix acknowledges that Company (or its third party auditors) may enter its premises for the purposes of conducting this audit, provided that Company gives it reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to Securonix's operations. Company will not exercise its audit rights more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority; or (ii) Company believes a further audit is necessary due to a Security Incident suffered by Securonix.

9.   **Data Transfers and Additional Safeguards**. To the extent that Securonix Processes Personal Data of Data Subjects located in or subject to the applicable Data Protection Laws of the European Economic Area ("EEA"), the United Kingdom, and/or Switzerland, by signing this Addendum, the Parties agree as follows:

10.   With respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of the Effective Date at https://ico.org.uk/media/for-

organisations/documents/4019539/international-data-transfer-addendum.pdf) ("UK SCCs") forms part of this Addendum and takes precedence over the rest of this Addendum as set forth in the UK SCCs, unless the United Kingdom issues updates to the UK SCCs that, upon notice from Customer, will control. Undefined capitalized terms used in this provision shall mean the definitions in the UK SCCs. For purposes of the UK SCCs, they shall be deemed completed as follows:

    i. Table 1 of the UK SCCs:

        1. The Parties' details shall be the Parties and their affiliates to the extent any of them is involved in such transfer.

        2. The Key Contact shall be the contacts set forth in the Agreement.

    ii. Table 2 of the UK SCCs: The Approved EU SCCs referenced in Table 2 shall be the EU SCCs as executed by the Parties.

    iii. Table 3 of the UK SCCs: Annex 1A, 1B, II, and III shall be set forth in Annexes I, II, and III below.

    iv. Table 4 of the UK SCCs: Either Party may end this Addendum as set out in Section 19 of the UK SCCs.

    v. By entering into this DPA, the Parties are deemed to be signing the UK SCCs, the Mandatory Clauses in Part 2, and its applicable Tables and Appendix Information.

10.1 For all other Personal Data, the EU SCCs form part of this DPA and take precedence over the rest of this DPA to the extent of any conflict.

10.2 With respect to Personal Data transferred from Switzerland for which Swiss law (and not the law in any EEA jurisdiction) governs the international nature of the transfer, references to the GDPR in Clause 4 of the EU SCCs are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority shall include the Swiss Federal Data Protection and Information Commissioner.

10.3 To the extent applicable, Securonix will provide reasonable assistance to Company for the parties' compliance obligations under Section III of the EU SCCs, including, to the extent legally permissible, by informing Company of new facts or determinations known to Securonix that are likely to negatively impact the level of protection that the transferred Personal Data receives.

10.4 Company and Securonix shall encrypt all transfers of the Personal Data between them, and Securonix shall encrypt any onward transfers it makes of such personal data, to prevent the acquisition of such data by third parties, such as governmental authorities who may gain physical access to the transmission mechanisms (e.g., wires and cables) while the data is in transmission.

10.5 Securonix represents and warrants that, as of the date of this contract, it has not received any directive under Section 702 of the U.S. Foreign Intelligence Surveillance Act, codified at 50 U.S.C. § 1881a ("FISA Section 702").

10.6 Securonix represents and warrants that no court has found Securonix to be the type of entity eligible to receive process issued under FISA Section 702: (i) an "electronic communication

service provider" within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition.

10.7   Securonix represents and warrants that it is not a "telecommunications carrier" as defined in 47 U.S.C. § 153.

10.8   Securonix will never comply with any request under FISA Section 702 for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific "targeted selector" (an identifier that is unique to the targeted endpoint of communications subject to the surveillance).

10.9   Securonix will use all reasonably available legal mechanisms to challenge any demands for data access through national security process it receives as well as any non-disclosure provisions attached thereto.

10.10   Securonix will take no action pursuant to U.S. Executive Order 12333.

10.11   No more than once in a twelve (12) month period, Company may request that Securonix provide a transparency report, available for review by Company, indicating the types of binding legal demands for personal data it has received, including national security orders and directives, which shall encompass any process issued under FISA Section 702.

10.12   Securonix will promptly notify Company if Securonix can no longer comply with the EU SCCs or UK SCCs, as applicable, or the clauses in this Section 10. Such notice shall entitle Company to terminate the Agreement (or, at Company's option, affected statements of work, order forms, and like documents thereunder) and receive a prompt pro-rata refund of any prepaid amounts thereunder. This is without prejudice to Company's other rights and remedies with respect to a breach of the Agreement.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

[Company]

Signature   _____

Name   _____

Title   _____

Date Signed   _____

Securonix, Inc.
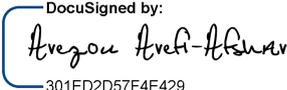
Signature   DocuSigned by:

Arezou Arefi-Afshar

301ED2D57F4E429...

Name   Arezou Arefi-Afshar

Title   General Counsel & Corporate Secretary

SCHEDULE A -- DATA PROCESSING ADDENDUM
EU STANDARD CONTRACTUAL CLAUSES

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the processing, including transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data processing and transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 - Clause 9 (a), (c), (d) and (e);

(iv) Clause 12 - Clause 12 (a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18 - Clause 18(a) and (b).
(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing

and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management, and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay, but not later than 48 hours after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 1 (one) month in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has

become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

> (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
> (ii) refer the dispute to the competent courts within the meaning of Clause 18.
> (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-

processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

14

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses. In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX
ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name:
Address:
Data Protection Officer's name, position, and contact details:
Activities relevant to the data transferred under these Clauses:

Signature:
Role:

Data importer(s):

1. Name: Securonix Inc.
Address: 5080 Spectrum Drive, Suite 950W, Addison, Texas 75001, USA
Data Protection Officer's name, position, and contact details: N/A
Activities relevant to the data transferred under these Clauses: Cybersecurity and security analytics products or support, the details of which are set out in greater detail in the Principal Agreement.

Signature:
Role: Processor
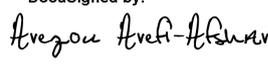
B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Categories of personal data transferred

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 for instance 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.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Nature of the processing

Purpose(s) of the data transfer and further processing

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

C. COMPETENT SUPERVISORY AUTHORITY

As indicated in Clause 13

SECURONIX DPA 2.2022

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Description of the technical and organisational security measures implemented by the data importer in accordance with Section 3.1 and 5:

Technical and Organizational Measures

a) Confidentiality

- Physical Access Control
  No unauthorized access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems

- Electronic Access Control
  No unauthorized use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media

- Internal Access Control (permissions for user rights of access to and amendment of data) No unauthorized Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorization concept, need-based rights of access, logging of system access events

- Isolation Control
  The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing;

b) Integrity

- Data Transfer Control
  No unauthorized Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;

- Data Entry Control
  Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

c) Availability and Resilience

- Availability Control
Prevention of accidental or willful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning

- Rapid Recovery

d) Procedures for Regular Testing, Assessment and Evaluation

- Data Protection Management;
- Incident Response Management;
- Data Protection by Design and Default
- Contract Control

No third-party data processing without corresponding instructions from the Client, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. Amazon Web Services
2. Crowdstrike
3. NXLog
4. Opora

SECURONIX DPA 2.2022