Openpath GDPR DATA PROCESSING ADDENDUM

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1 Purpose and Scope

Purpose - 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) (GDPR) for the transfer of data to a third country.

Scope - This DPA applies when Customer Data is processed by OPENPATH. In this context, OPENPATH will act as "processor" to Customer who may act either as "controller" or "processor" with respect to Customer Data (as each term is defined in the GDPR).

The entity identified as "Customer" in (the "data exporter", "controller") as below

Customer Name: _____

Customer Address: _____

and

Openpath Security, Inc.
13428 Maxella Ave, #866, Marina Del Rey, CA 90292, USA.
(the "**data importer", "processor"**) each a "party"; together "the parties"),

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in this agreement.

Definitions

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the

protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter*' means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

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 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 8.1(b), 8.9(a), (c), (d) and (e);

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

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) 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.

SECTION II – OBLIGATIONS OF THE PARTIES

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 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 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 ([i]) (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, under the appropriate Module, 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 non-compliance. 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) GENERAL WRITTEN AUTHORISATION 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 30 days 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. ([ii]) 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) [Where the data exporter is established in an EU Member State:] 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.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

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]);

(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 by 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.

(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.

SECTION IV – FINAL PROVISIONS

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 Ireland.

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 Ireland.

(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.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

The entity identified as "Customer" in the DPA (the "**data exporter**", "controller")

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

A company established in the European Union that wishes to obtain software and hardware solutions and related services from the data importer.

Signature and date: _____

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: Openpath Security, Inc.

Address: 13428 Maxella Ave, #866, Marina Del Rey, CA 90292, USA. (the "**data importer", "processor"**)

Contact person's name, position and contact details: _____

___John Kim, Senior Director of Product, dpo@openpath.com_____

Activities relevant to the data transferred under these Clauses:

A company that provides software and hardware solutions and related services form the data importer.

Signature and date: _____

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The data subjects may include Customer's customers, employees, suppliers and end-users.

Categories of personal data transferred

End user data includes name, email address, profile picture (optional), mobile device and log information, entry time stamp, Bluetooth signal, Technical Support feedback information, end user data in audit logs **and any additional optional data submitted by controller.**

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).

The data will be continuously transferred

Nature of the processing

Logging, reporting and such other Services as described in the Documentation and initiated by Customer from time to time.

Purpose(s) of the data transfer and further processing

The purpose of the data processing under this DPA is the provision of the Services initiated by Customer.

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

The duration of the data processing under this DPA is two years from collection of the data.

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

…

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The parties identify the Irish Supervisory Authority – the Data Protection Commission as the competent supervisory authority in accordance with Clause 13

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. Customer Instructions. The parties agree that this DPA and the Agreement (including the provision of instructions via configuration tools such as the Openpath Control Portal and APIs made available by OPENPATH for the Services) constitute Customer's documented instructions regarding OPENAPTH's processing of Customer Data ("Documented Instructions"). OPENPATH will process Customer Data only in accordance with Documented Instructions. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between OPENPATH and Customer, including agreement on any additional fees payable by Customer to OPENPATH for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if OPENPATH declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA.

2. Confidentiality of Customer Data. OPENPATH will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends OPENPATH a demand for Customer Data, OPENPATH will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, OPENPATH may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then OPENPATH will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless OPENPATH is legally prohibited from doing so. If the Standard Contractual Clauses apply, nothing in this Section 3 varies or modifies the Standard Contractual Clauses.

3. Confidentiality Obligations of OPENPATH Personnel. OPENPATH restricts its personnel from processing Customer Data without authorization by OPENPATH as described in the OPENPATH Information Security Policy. OPENPATH imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

4. Security of Data Processing. OPENPATH has implemented and will maintain security measures for the OPENPATH Network as described in the OPENPATH Security Policy and this Section. In particular, OPENPATH has implemented and will maintain the following technical and organizational measures:

(a) security of the OPENPATH Network in accordance with the NIST Cloud Security Framework;

(b) physical security of the facilities as set out in the OPENPATH Technical and Organizational Security Measures document;

(c) measures to control access rights for OPENPATH employees and contractors in relation to the OPENPATH Network as set out in the OPENPATH Technical and
Organizational Security Measures document; and

(d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by OPENPATH as described in the OPENPATH Security Policy.

5.2 Customer may elect to implement technical and organizational measures in relation to Customer Data. Such technical and organizational measures include the following which may be obtained by Customer from OPENPATH as described in the Documentation, or directly from a third party supplier:

(a) anonymization of user data to ensure an appropriate level of security and privacy;

(b) measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are being operated by Customer;

(c) measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and

(d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

(e) Using multi-factor authentication in accessing the OPENPATH control centre for added security.

6. Sub-processing.

This section is applicable only is so far as it does not override the specific requirement of clause 9.

6.1 Authorized Sub-processors. Customer agrees that OPENPATH may use subprocessors to fulfil its contractual obligations under this DPA or to provide certain services on its behalf, such as providing support services. Customer consents to OPENPATH's use of sub-processors as described in this Section. Except as set forth in this Section, or as Customer may otherwise authorize, OPENPATH will not permit any sub-processor to carry out processing activities on Customer Data on behalf of Customer.

6.2 Sub-processor Obligations. Where OPENPATH authorizes any sub-processor as described in Section 6.1:

(i) OPENPATH will restrict the sub-processor's access to Customer Data only to what is necessary to maintain the Services or to provide the Services to Customer and any End Users in accordance with the Documentation and OPENPATH will prohibit the sub-processor from accessing Customer Data for any other purpose;

(ii) OPENPATH will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the sub-processors that cause OPENPATH to breach any of OPENPATH's obligations under this DPA.

7. Data Subject Rights

Taking into account the nature of the Services, OPENPATH offers Customer certain controls as described in Sections 1.2 and 5.2 that Customer may elect to use to comply with its obligations towards data subjects. Should a data subject contact OPENPATH with regard to correction or deletion of its personal data, OPENPATH will use commercially reasonable efforts to forward such requests to Customer.

8. **Optional Security Features.** OPENPATH makes available a number of security features and functionalities that Customer may elect to use. Customer is responsible for (a) implementing the measures described in Section 5.2, as appropriate, (b) properly configuring the Services, (c) using the controls available in connection with the Services (including the security controls) to allow Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (e.g. backups and routine archiving of Customer Data), and (d) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorized access and measures to control access rights to Customer Data.

9. **Security Breach Notification.**

9.1 Security Incident. OPENPATH will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

9.2 OPENPATH Assistance. To assist Customer in relation to any personal data breach notifications Customer is required to make under the GDPR, OPENPATH will include in the notification under section 9.1(a) such information about the Security Incident as OPENPATH is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to OPENPATH, and any restrictions on disclosing the information, such as confidentiality.

9.3 Unsuccessful Security Incidents. Customer agrees that:

(i) an unsuccessful Security Incident will not be subject to this Section 9. An unsuccessful Security Incident is one that results in no unauthorised access to

Customer Data or to any of OPENPATH's equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents; and

(ii) OPENPATH's obligation to report or respond to a Security Incident under this Section 9 is not and will not be construed as an acknowledgement by OPENPATH of any fault or liability of OPENPATH with respect to the Security Incident.

9.4 Communication. Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means OPENPATH selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the OPENPATH management console and secure transmission at all times.

10. **OPENPATH Certifications and Audits.**

10.1 OPENPATH Audits. OPENPATH uses external auditors to verify the adequacy of its security measures, including the security of the physical data centres from which OPENPATH provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to SOC 2 standards or such other alternative standards that are substantially equivalent to SOC 2; (c) will be performed by independent third party security professionals at OPENPATH's selection and expense; and (d) will result in the generation of an audit report ("**Report**"), which will be OPENPATH's Confidential Information.

10.2 Privacy Impact Assessment and Prior Consultation. Taking into account the nature of the Services and the information available to OPENPATH, OPENPATH will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation pursuant to Articles 35 and 36 of the GDPR, by providing the information OPENPATH makes available under this Section 10.

11. **Customer Audits.** Customer agrees to exercise any right it may have to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by instructing OPENPATH to carry out the audit described in Section 10. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending OPENPATH written notice as provided for in the Agreement. If OPENPATH declines to follow any instruction requested by Customer regarding audits or inspections, Customer is entitled to terminate this DPA and the Agreement. If the Standard Contractual Clauses apply, nothing in this Section varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.
12. **Transfers of Personal Data.**

12.1 Application of Standard Contractual Clauses. The Standard Contractual Clauses will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR). The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply if OPENPATH has adopted Binding Corporate Rules for Processors or an alternative recognised compliance standard for the lawful transfer of personal data (as defined in the GDPR) outside the EEA.

12.2 If OPENPATH is required by law or in response to a competent regulatory or government agency to disclose or surrender personal data transferred by Customer, OPENPATH will (to the extent legally possible) not provide the personal data until instructed to do so by Customer and will notify Customer with enough:

(a) information; and
(b) notice,

to enable Customer to challenge the legal or competent regulatory or government agency requirement and will provide Customer with all the cooperation and assistance as reasonably required.

12.3 Where OPENPATH fails to comply with this Agreement, or where, despite this Agreement, a level of protection essentially equivalent to that guaranteed by the Data Protection Legislation (in the reasonable opinion of the Customer) cannot be ensured, Customer may suspend or terminate transfers of personal data to OPENPATH located in a Third Country, and Customer may terminate the Service in whole or in part on 30 days' prior written notice at no additional cost and without further liability either, and where fees for the Services are paid in advance, it shall be entitled to a prorated refund in respect of fees paid for Services not provided in accordance with the Agreement as at the effective date of termination.

12.4 The parties acknowledge and agree that the Standard Contractual Clauses may not, in isolation, ensure that OPENPATH'S processing complies with the international transfer requirements and, the parties agree to cooperate with each other in good faith to agree to written variations to this Agreement, and to take such action as may reasonably be required, to ensure that such processing complies with the international transfer requirements. To the extent that Customer determines that the processing cannot comply with the international transfer requirements, Customer may at no additional cost and without further liability either:

12.4.1 request OPENPATH to evaluate the feasibility of processing personal data within certain jurisdictions subject to certain restrictions, supplementary measures and/or safeguards; and/or

12.4.2 terminate the Service in whole or in part on 30 days' prior written notice and where fees for the Service are paid in advance, it shall be entitled to a prorated

refund in respect of fees paid for Service not provided in accordance with the Agreement as at the effective date of termination.

13. **Termination of the DPA.** This DPA shall continue in force until the termination of the Agreement (the "Termination Date").
14. **Return or Deletion of Customer Data.** The Services provide Customer with controls that Customer may use to retrieve or anonymize Customer Data as described in the Documentation. Up to the Termination Date, Customer will continue to have the ability to retrieve or anonymize Customer Data in accordance with this Section.
15. **Duties to Inform.** Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by OPENPATH, OPENPATH will inform Customer without undue delay. OPENPATH will, without undue delay, notify all relevant parties in such action (e.g. creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.
16. **Entire Agreement; Conflict.** Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the parties

    including the Agreement and this DPA, the terms of this DPA will control, except that the Service Terms will control over this DPA.
17. **Definitions.** Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below:

    "OPENPATH Network" means compute, storage, processing, and delivery services provided to OPENPATH by cloud service provides such as AWS, Microsoft, Google, and or others as necessary to provide the Services.

    "Customer" means you or the entity you represent.
    "Customer Data" means the "personal data" (as defined in the GDPR) that is uploaded to the Services under Customer's OPENPATH accounts.

    "EEA" means the European Economic Area.

    "GDPR" means Regulation 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

    "processing" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

    "Security Incident" means a breach of OPENPATH's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

"Standard Contractual Clauses" means Annex 2, attached to and forming part of this DPA pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC.

"Third Country" means a country who is not a member of the EEA that has not been the subject of a finding of an adequate level of protection by the European Commission (or the relevant UK authority in relation to sharing personal data outside the UK.

OPENPATH Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1. Information Security Program. OPENPATH will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the OPENPATH Network, and (c) minimize security risks, including through risk assessment and regular testing.

1.1 Network Security. The OPENPATH Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. OPENPATH will maintain access controls and policies to manage what access is allowed to the OPENPATH Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. OPENPATH will maintain corrective action and incident response plans to respond to potential security threats.

1.2 Physical Security

1.2.1 Physical Access Controls. Physical components of the OPENPATH Network are housed at cloud service providers such as AWS, Microsoft, or Google. OPENPATH has reviewed their security, privacy and compliance programs to ensure it meets OPENPATH requirements.

1.2.2 Limited Employee and Contractor Access. OPENPATH provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of OPENPATH or its Affiliates.

1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. OPENPATH also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. Continued Evaluation. OPENPATH will conduct periodic reviews of the security of its OPENPATH Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. OPENPATH will continually evaluate the security of its OPENPATH Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

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

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

2. …

---

[i] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[ii] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[iii] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.