DATA PROCESSING ADDENDUM

1. BACKGROUND

1.1 This Data Processing Addendum ("**DPA**") is entered into by and between Customer and PolyOps and forms a part of the Customer Terms and Conditions entered into by the Parties (the "**Agreement**") and is incorporated therein upon execution.

2. INTERPRETATION

2.1 Unless otherwise defined below, each capitalized term in this DPA shall have the meaning set out in the Agreement.

(a) "**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., including any amendments and any implementing regulations thereto that become effective on or after the effective date of this DPA;

(b) "**Controller**" means the entity which, along or jointly with others, determines the purposes and means of the Processing of personal information;

(c) "**Customer Personal Information**" means the personal information that PolyOps Processes on behalf of the Customer in connection with PolyOps's provision of the Services, as more particularly described in ANNEX 1;

(d) "**Data Protection Laws**" means any legislation protecting the fundamental rights and freedoms of persons and their rights to privacy with regard to the Processing of personal information, including without limitation the GDPR (and any national legislation implementing or supplementing the GDPR), the UK Data Protection Act 2018 and the CCPA;

(e) "**European Economic Area**" or "**EEA**" means the Member States of the European Union together with the UK, Iceland, Norway, and Liechtenstein;

(f) "**GDPR**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council and/or (where applicable) the "UK GDPR" as defined in The Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit) Regulations 2019;

(g) "**personal information**" means any information relating to an identified or identifiable individual (a "**data subject**");

(h) "**Processing**" means any operation or set of operations which is performed on personal information, or on sets of personal information, whether or not by automated means, and "**Process**" will be interpreted accordingly;

(i) "**Processor**" means the entity that Processes personal information on behalf of a controller;

(j) "**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Customer Personal Information;

(k)   "**Sell**" shall have the meaning given in the CCPA;

(l)   **"Services"** means the service(s) provided by PolyOps to Customer under the Agreement**;**

(m)   "**Standard Contractual Clauses**" means the Standard Contractual Clauses (processors) approved by the European Commission Decision C(2010)593 and set out in ANNEX 4, or any subsequent version thereof released by the European Commission (which will automatically apply); and

(n)   "**Subprocessor**" means any Processor engaged by PolyOps who agrees to receive from PolyOps Customer Personal Information.

3.   DATA PROCESSING

3.1   **Role of the Parties.** The Parties acknowledge and agree that:

(a)   for the purposes of the GDPR, PolyOps acts as Processor and the Customer acts as Controller; and

(b)   for the purposes of the CCPA, PolyOps will act as a "Service Provider" (as such term is defined in the CCPA), in its performance of its obligations pursuant to the Agreement.

3.2   **Instructions for Data Processing.** PolyOps will, subject to clause 3.3, only Process Customer Personal Information in accordance with:

(a)   the Agreement, to the extent necessary to provide the Services to Customer; and

(b)   Customer's written instructions.

Notwithstanding the foregoing, nothing in this DPA shall restrict PolyOps's ability to Process Customer Personal Information in de-identified or anonymous format.

3.3   PolyOps may Process Customer Personal Information to the extent required by applicable laws to which PolyOps is subject.

3.4   The Customer shall provide all applicable notices to data subjects required under applicable Data Protection Laws for the lawful Processing of Customer Personal Information by PolyOps in accordance with the Agreement.

3.5   The Customer will obtain any consents required under applicable Data Protection Laws for the lawful Processing of Customer Personal Information by PolyOps in accordance with the Agreement.

3.6   The Customer agrees to defend, indemnify and keep indemnified, and hold harmless, at its own expense, PolyOps against all costs, claims, damages and expenses incurred by PolyOps or for which PolyOps may become liable due to any failure by the Customer to comply with clause 3.4 and clause 3.5.

3.7   The Customer acknowledges that PolyOps is reliant on the Customer for direction as to the extent to which PolyOps is entitled to use and process the Customer Personal Information. Consequently, PolyOps will not be liable for any claim brought against the Customer by a data subject arising from any act or omission by PolyOps to the extent that such act or omission resulted from the Customer's instructions or the Customer's use of the Services.

4.   SUBPROCESSORS

4.1   **Consent to Subprocessor Engagement**. The Customer generally authorises the engagement of third parties as Subprocessors.

4.2   **Information about Subprocessors**. A current list of PolyOps Subprocessors is available in Annex 3 ("**Subprocessor List**"), which may be updated by PolyOps from time to time in accordance with clause 4.3, and following the notice provision in clause 13.4

4.3   **Requirements for Subprocessor Engagement**. When engaging any Subprocessor, PolyOps will:

(a)   ensure via a written agreement that:

(i)   the Subprocessor only accesses and uses Customer Personal Information to the extent required to perform the obligations subcontracted to it and does so in accordance with this DPA; and

(ii)   substantially similar obligations are imposed on the Subprocessor with regard to their Processing of Customer Personal Information, as are imposed on PolyOps under this DPA; and

(b)   remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

4.4   **Opportunity to Object to Subprocessor Changes.**

(a)   Customer may, on reasonable grounds, object to PolyOps's use of a new Subprocessor by providing PolyOps with written notice within fifteen (15) days after PolyOps has provided notice to the Customer as described in clause 4.2.

(b)   Customer may object to the appointment of that Subprocessor, on reasonable grounds, by providing documentary evidence that reasonably shows that the Subprocessor does not or cannot comply with the requirements in this DPA ("**Objection**"). In the event of an Objection, PolyOps will use reasonable endeavours to make available to the Customer a change in the Services or will recommend a commercially reasonable change to the Services to prevent the applicable Subprocessor from Processing the Customer Personal Information. If PolyOps is unable to make available such a change within a reasonable period of time, which shall not exceed thirty (30) days, either Party may terminate, without penalty, the Agreement by providing written notice to the other Party.

5.   INTERNATIONAL TRANSFERS

5.1   To the extent that Customer Personal Information from Customer's establishments in the EEA is exported to, or accessed by PolyOps from outside the EEA, such transfers will be governed by the Standard Contractual Clauses set forth at ANNEX 4.

5.2   In the event of a conflict between any of the provisions of the Standard Contractual Clauses and this DPA, the provisions of the Standard Contractual Clauses shall prevail.

5.3   The Customer has, with respect to such transfers of Customer Personal Information in accordance with clause 5.1, satisfied itself that PolyOps is able to provide a level of protection for such Customer Personal Information that is essentially equivalent to the protection afforded to such Customer Personal Information under EEA law.

6.   PROCESSING OF CCPA PERSONAL INFORMATION

6.1   The following provisions apply to Customer Personal Information subject to the CCPA:

(a)   **Processing of Customer Personal Information.** PolyOps shall not collect, process, or retain Customer Personal Information for any purpose other than the specific purpose of providing the Services to Customer pursuant to the Agreement. PolyOps acknowledges and agrees that it shall not retain, use or disclose CCPA Personal Information for a commercial purpose other than providing the Services. Notwithstanding the foregoing, nothing in this DPA shall restrict PolyOps's ability to Process Customer Personal Information to comply with applicable laws or as otherwise permitted by the CCPA.

(b)   **Disclosure of Customer Personal Information**. PolyOps shall not Sell, disclose, release, transfer, make available or otherwise communicate any Customer Personal Information to another business or third party without the prior written consent of Customer unless and to the extent that such disclosure is made to a Subprocessor for a business purpose. Notwithstanding the foregoing, nothing in this DPA shall restrict PolyOps's ability to disclose Customer Personal Information to comply with applicable laws or as otherwise permitted by the CCPA.

7.   DATA SECURITY, AUDITS AND SECURITY NOTIFICATIONS

7.1   **PolyOps Security Obligations**. PolyOps shall implement appropriate technical and organizational measures to protect the Customer Personal Information to ensure a level of security appropriate to the risk. Without limiting the generality of the foregoing, PolyOps shall put in place and maintain the technical and organizational measures as set out in ANNEX 2 of this DPA.

7.2   **Security Audits**. To the extent expressly required in writing by a competent data protection authority or following a Security Incident involving Customer Personal Information, the Customer may, upon reasonable notice and at reasonable times, audit (either by itself or using independent third party auditors) PolyOps's compliance with the security measures set out in this DPA (including the technical and organisational measures as set out in ANNEX 2).

Guidance shall assist with, and contribute to, any audits conducted in accordance with this clause 7.2.

7.3   **Security Incident Notification.** If PolyOps becomes aware of a Security Incident, then PolyOps shall promptly notify the Customer, take any additional steps that are reasonably necessary to remedy any non-compliance with this DPA, including complying with all applicable requirements of the Agreement, and reasonably cooperate in the investigation of the Security Incident.

7.4   **PolyOps Employees and Personnel.** PolyOps shall limit access to Customer Personal Information to those employees or other personnel who have a business need to have access to such Customer Personal Information. Further, PolyOps shall ensure that such employees or other personnel are subject to a duty of confidentiality with respect to the Customer Personal Information.

7.5   **Government Disclosure.** PolyOps shall promptly notify the Customer of any request for the disclosure of Customer Personal Information by a governmental or regulatory body or law enforcement authority (including any data protection supervisory authority) unless otherwise prohibited by law or a legally binding order of such body or agency.

8.   ACCESS REQUESTS AND DATA SUBJECT RIGHTS

8.1   **Data Subject Requests**. Unless otherwise required by applicable law, PolyOps shall promptly notify Customer of any request received by PolyOps or any Subprocessor from a data subject in respect of the Customer Personal Information and shall not respond to the data subject.

8.2   PolyOps shall, where possible, assist Customer with ensuring its compliance under applicable Data Protection Laws by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising data subject rights laid down in the Data Protection Laws and in particular shall:

        (a)   provide Customer with the ability to correct, delete, block, access, or copy the Customer Personal Information, or

        (b)   promptly correct, delete, block, access, or copy Customer Personal Information within the Services at Customer's request.

9.   DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

9.1   PolyOps shall provide reasonable assistance to Customer with any data protection impact assessments and with any prior consultations to any regulatory authority of Customer which are referred, in each case solely in relation to Processing of Customer Personal Information and taking into account the nature of the Processing and information available to PolyOps.

10.   RETURN AND DELETION

10.1   **Deletion of data**. Subject to clause 10.2 below, PolyOps shall, within sixty (60) days of the date of termination of the Agreement:

(a) if requested to do so by the Customer, return a copy of all Customer Personal Information by secure file transfer in such a format as notified by the Customer to PolyOps; and

(b) delete and use all reasonable efforts to procure the deletion of all other copies of Customer Personal Information Processed by PolyOps or any Subprocessors.

10.2 PolyOps and its Subprocessors may retain Customer Personal Information to the extent required by applicable laws and only to the extent and for such period as required by applicable laws and always provided that PolyOps shall ensure the confidentiality of all such Customer Personal Information and shall ensure that such Customer Personal Information is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

IN WITNESS WHEREOF, the Parties hereto have duly executed this DPA as of the Effective Date.

PolyOps, Inc.   **Customer**

By: _____   By: _____

Print Name: _____   Print Name: _____

Title: _____   Title: _____

Date: _____   Date: _____

ANNEX 1 - DETAILS OF THE PROCESSING OF CUSTOMER PERSONAL INFORMATION

This ANNEX 1 includes certain details of the Processing of Customer Personal Information as required by Article 28(3) of the GDPR.

Subject matter and duration of the Processing of Customer Personal Information

- The subject matter of the data processing under this DPA is Customer Personal Information.

The nature and purpose of the Processing of Customer Personal Information

- Storing and processing Customer Personal Information in connection with the PolyOps Services.

- The duration of the data processing under this DPA is determined in accordance with the Agreement.

The types of Customer Personal Information to be processed

- Consumer data from the Customer may include name, email, address, IP address, device ID, location

The categories of data subject to whom the Customer Personal Information relates

- Data subjects may include Customer's end users.

Customer's obligations and rights

- The Customer's obligations and rights are set out in the Agreement.

ANNEX 2

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

1. PolyOps maintains internal policies and procedures, or procures that its Subprocessors do so, which are designed to:

    (a)   secure any personal data Processed by PolyOps against accidental or unlawful loss, access or disclosure;

    (b)   identify reasonably foreseeable and internal risks to security and unauthorized access to the personal data Processed by PolyOps;

    (c)   minimize security risks, including through risk assessment and regular testing.

2. PolyOps will—and will use reasonable efforts to procure that its Subprocessors will—conduct periodic reviews of the security of their network and the adequacy of their information security program as measured against industry security standards and its policies and procedures.

3. PolyOps will—and will use reasonable efforts to procure that its Subprocessors will— periodically evaluate the security of their 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 3

SUBPROCESSOR LIST

Amazon Web Services
Google Cloud
Datadog
CircleCI
LayerCI
Sentry
GitHub
Segment
FullStory
Fivetran
Census
Customer.io
Metabase
Google Analytics
Heap
Stripe
Bill.com
Sendgrid
Twillio
Slack
Cloudlfare
Hubpsot

ANNEX 4

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of this ANNEX 4, references to the "data exporter" and "data importer" shall be to the Customer and to PolyOps respectively (each a "*party*"; together "*the parties*").

Clause 1

Definitions

For the purposes of the Clauses:

(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

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix A which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the

entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix B to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect 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, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix B, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a)   to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b)   that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c)   that it has implemented the technical and organisational security measures specified in Appendix B before processing the personal data transferred;

(d)   that it will promptly notify the data exporter about:

     (i)   any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

     (ii)   any accidental or unauthorised access, and

     (iii)   any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e)   to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f)   at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g)   to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix B which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h)   that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i)   that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j)   to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1.   The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2.   If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of

any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3.   If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1.   The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a)   to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b)   to refer the dispute to the courts in the Member State in which the data exporter is established.

2.   The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1.   The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2.   The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3.   The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1.   The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2.   The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.   The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4.   The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1.   The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2.   The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX A

Data exporter

The data exporter is the Customer

Data importer

The data importer is PolyOps

Data subjects

The personal data transferred concern the categories of data subjects identified in ANNEX 1 to this DPA

Categories of data

The personal data transferred concern the categories of data identified in ANNEX 1 to this DPA.

Processing operations

The personal data transferred will be subject to the following basic processing activities: transmitting, collecting, storing and analysing data in connection with the provision of the Services.

APPENDIX B

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The data importer implements the technical and organisational security measures identified in ANNEX 2 to this DPA.