DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms a part of the Customer Terms of Use or any other agreement pertaining to the delivery of the Services, including without limitation any “Order Form” or “Sales Order" (the "**Agreement**") between Strigo Ltd. ("**Strigo**") and the Customer named in such Agreement to reflect the parties’ agreement with regard to the Processing of Personal Data (as those terms are defined below).

In the course of providing the Services under the Agreement, Strigo may Process certain Personal Data (such terms defined below) on behalf of Customer and where Strigo Processes such Personal Data on behalf of Customer, the Parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

By signing the DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Controller Affiliates (defined below). For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Controller Affiliates.

If the entity signing this DPA is not a party to an effective Agreement with Strigo, this DPA shall not be valid or legally binding. In the event of a conflict between the terms and conditions of this DPA and the Agreement, the terms and conditions of this DPA shall supersede and control to the extent of such conflict.

HOW TO EXECUTE THIS ADDENDUM:

1. This Addendum (and Standard Contractual Clauses in Exhibit B, if applicable) may have been pre-signed on behalf of Strigo as the data importer.

2. To complete this Addendum, Customer must:

a. Complete the information in the signature box and sign on Pages 5, 13 and 15.

b. Complete the information as the data exporter on Pages 7 and 13.

3. Send the completed and signed Addendum to Strigo by email, indicating the Customer’s Legal Name, to privacy@strigo.io. Upon receipt of the validly completed Addendum by Strigo at this email address, this Addendum will become legally binding.

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. DEFINITIONS

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

“**Anonymous Data**” means Personal Data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable natural person.

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Controller Affiliate**" means any of Customer's Affiliate(s) (a) (i) that are subject to applicable Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (ii) permitted to use the Services pursuant to the Agreement between Customer and Strigo, but have not signed their own Order Form and are not a "Customer" as defined under the Agreement, (b) if and to the extent Strigo processes Personal Data for which such Affiliate(s) qualify as the Controller.

"**Data Protection Laws**" means all laws and regulations, including laws and binding regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates. Data Subjects include the individuals about whom data is provided to Strigo via the Services by or at the direction of the Customer, including natural persons who submit personal data to Customer via use of the Services (including Participants and Team Members and all Event communication hosted by Strigo on behalf of Customer).

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

"**Personal Data**" means any information relating to Data Subject which Processor Processes on behalf of Controller other than Anonymous Data, and includes Sensitive Personal Information.

“**Personal Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

"**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller.

“**Sensitive Personal Information**” means a Data Subject’s (i) government-issued identification number (including social security number, driver’s license number or state-issued identification number); (ii) financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual’s financial account; (iii) genetic and biometric data or data concerning health; or (iv) Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation or sexual activity, criminal convictions and offences (including commission of or proceedings for any offense committed or alleged to have been committed), or trade union membership.

"**Standard Contractual Clauses**" means the agreement executed by and between Customer and Strigo and attached hereto as Exhibit C pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"**Sub-processor**" means any entity engaged by Strigo to Process Personal Data in connection with the Services.

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties**. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller and Strigo is the Processor.

2.2 **Customer's Processing of Personal Data.** Customer shall, in its use of the Services and provision of instructions, Process Personal Data in accordance with the requirements of applicable Data Protection Law. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3 **Strigo's Processing of Personal Data.** As Customer's Processor, Strigo shall only Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Team Members in their use of the Services; and (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) that are consistent with the terms of the Agreement (individually and collectively, the "**Purpose**"). Strigo acts on behalf of and on the instructions of Customer in carrying out the Purpose.

2.4 **Details of the Processing**. The subject-matter of Processing of Personal Data by Strigo is as described in the Purpose in Section 2.3 above. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Exhibit B (Description of Processing Activities) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Requests**. Strigo shall, to the extent legally permitted, promptly notify Customer if Strigo receives any requests from a Data Subject to exercise the following Data Subject rights in relation to Personal Data: access, rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, or to not be subject to an automated individual decision making (each, a "**Data Subject Request**"). Taking into account the nature of the Processing, Strigo shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under applicable Data Protection Laws. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Strigo shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Strigo is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Strigo's provision of such assistance, including any fees associated with provision of additional functionality.

4. SUB-PROCESSORS

4.1 **Appointment of Sub-processors**. Customer acknowledges and agrees that Strigo may engage third-party Sub-processors in connection with the provision of the Services. As a condition to permitting a third-party Sub-processor to Process Personal Data, Strigo will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor. In addition, Strigo shall post a list of its Sub-processors (if any) on the Site, as such list may be amended from time to time.

4.2 **Objection Right for Sub-processors**. Customer may reasonably object to Strigo's use of a certain Sub-processor (e.g., if making Personal Data available to the Sub-processor may violate applicable Data Protection Law or weaken the protections for such Personal Data) by notifying Strigo promptly in writing within ten (10) business days after receipt of Strigo's notice in connection therewith. Such notice shall explain the reasonable grounds for the objection. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Strigo will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Strigo is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate without penalty the applicable Order Form(s) with respect only to those Services which cannot be provided by Strigo without the use of the objected-to new Sub-processor by providing written notice to Strigo. Strigo will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

4.3 **Liability**. Strigo shall be liable for the acts and omissions of its Sub-processors to the same extent Strigo would be liable if performing the Services of each Sub-processor directly under the terms of this DPA.

5. SECURITY OF PERSONAL DATA

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data, including, but not limited to, the security measures set out in Appendix 2 to the Standard Contractual Clauses.

5.2 The Processor shall implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

5.2.1 the pseudonymisation and encryption of personal data;

5.2.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5.2.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

5.2.4 a process for regularly testing, assessing and evaluating the effectiveness of security measures.

6. PERSONAL DATA BREACH

6.1 In the event of a Personal Data Breach, Processor shall, without undue delay but no later than forty-eight (48) hours after confirming that a breach of personal data has occurred, inform Controller of the Personal Data Breach and take such steps as Processor in its sole discretion deems necessary and reasonable to remediate such violation.

6.2 In the event of a Personal Data Breach, Processor shall, taking into account the nature of the Processing and the information available to Processor, provide Controller with reasonable cooperation and assistance necessary for Controller to comply with its obligations under Applicable Data Protection Law with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

6.3 The obligations described in Sections 6.1 and 6.2 above shall not apply in the event that a Personal Data Breach results from the actions or omissions of Controller. Processor's obligation to report or respond to a Personal Data Breach under Sections 6.1 and 6.2 above will not be construed as an acknowledgement by Processor of any fault or liability with respect to the Personal Data Breach

7. RETURN AND DELETION OF PERSONAL DATA

Upon termination of the Services for which Strigo is Processing Personal Data, Strigo shall, upon Customer's request, and subject to the limitations described in the Agreement, return all Personal Data in Strigo's possession to Customer or securely destroy such Personal Data and demonstrate to the satisfaction of Customer that it has taken such measures, unless applicable law prevents it from returning or destroying all or part of Personal Data.

8. EUROPEAN SPECIFIC PROVISIONS

8.1 **GDPR**. Strigo will Process Personal Data in accordance with the GDPR requirements directly applicable to Strigo's provisioning of the Services.

8.1.1 **Data Protection Impact Assessment**. Upon Customer's request, Strigo shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Strigo. Strigo shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority, to the extent required under the GDPR.

8.2 **Transfer Mechanisms**. Strigo self-certifies to and complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, as administered by the US Department of Commerce. For transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states and Switzerland to countries which do not ensure an adequate level of data protection within the meaning of applicable Data Protection Laws of the foregoing territories, to the extent such transfers are subject to such applicable Data Protection Laws:

Strigo's EU-U.S. and Swiss-U.S. Privacy Shield Framework self-certifications apply; and

The Standard Contractual Clauses set forth in Exhibit B to this DPA apply.

Customer

Signature: ……………………………...…..

Customer Legal Name: …………………

Print Name: ……………………………..

Title: …………………………………….

Date: …………………………………….

Strigo Ltd.

Signature: Amit Cohen

Print Name: Amit Cohen

Title: Data Protection Officer

Date: 09/19/2019

EXHIBIT A

DESCRIPTION OF PROCESSING ACTIVITIES

Nature and Purpose of Processing: Processor will Process Personal Data on behalf of Controller for the purposes of providing the Services in accordance with the Agreement.

Duration of Processing: The term of the Agreement plus the period until Processor deletes all Personal Data processed on behalf of Controller in accordance with the Agreement.

Categories of Data Subjects: Individuals about whom Personal Data is provided to Processor via the Services by (or at the direction of) Controller or Controller's end users, which may include without limitation Controller's employees, contractors and end users.

Type of Personal Data: Personal Data provided to Processor via the Services by (or at the direction of) Controller or Controller's end users, including but not limited to the following:

User Profile: First Name, Last Name, Phone (optional), Email, Password (if SSO is not used), Profile Picture (optional), Department (optional).

Event Metadata: Topic, Description (optional), Participant IP addresses, device/hardware information.

EXHIBIT B

STANDARD CONTRACTUAL CLAUSES

Customer should complete and execute Exhibit B if it will transfer Personal Data to Strigo directly from a member state of the European Union, Iceland, Liechtenstein, Norway, Switzerland or the United Kingdom . This Exhibit cannot be modified in any way.

Please leave Exhibit B blank (and DO NOT SIGN) if Customer's use of Strigo's services will not involve Customer transferring Personal Data to Strigo from any of the countries mentioned above.

Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: ………………………………………………………………..

Address:....……………………………………..………………………………………….…………

Tel.: ………………………...…….…………….; fax: …………………………....……………….;

e-mail: ……………………………………….

Other information needed to identify the organisation:

……………………………………………

(the data exporter)

And

Name of the data importing organization: Strigo Ltd.

Address: 12 Carlebach St., Tel Aviv, Israel

Tel.: none; fax: none; e-mail: privacy@strigo.io

Other information needed to identify the organisation: not applicable

Amit Cohen

(the data importer)

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 Appendix 1.

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 Controller;

(c) 'the data importer' means Processor;

(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 organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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 1 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 2 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 2, 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 2 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 2 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 Clauses1. 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.

On behalf of the data exporter:

Name (written out in full): ……………………………………………….………………..

Position: …………………………………………….……………...

Address: …………………………………………….……………..

Other information necessary in order for the contract to be binding (if any):

Signature ………………………………

(stamp of organization)

On behalf of the data importer:

Name (written out in full): Amit Cohen

Position: Data Protection Officer

Address: 12 Carlebach St., Tel Aviv, Israel

Other information necessary in order for the contract to be binding (if any): not applicable

Signature Amit Cohen

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is a customer or other user of the data importer's communication software, services, systems and/or technologies.

Data importer

The data importer is a provider of communication software, services, systems and/or technologies.

Data subjects

Individuals about whom data is provided to Processor via the Services by (or at the direction of) Controller or Controller's end users, including without limitation Controller's employees, consultants, contractors, agents, and end users

Categories of data

Any Personal Data provided to Strigo via the Services, by (or at the direction of) Customer or Customer's end users, including but not limited to the following:

User Profile: First Name, Last Name, Phone (optional), Email, Password (if SSO is not used), Profile Picture (optional), Department (optional)

Meeting Metadata: Topic, Description (optional), participant IP addresses, device/hardware information

Cloud Recordings (optional): Mp4 of all video, audio and presentations, M4A of all Audio, Text file of all in meeting chats, Audio transcript file

IM Chat Logs

Telephony Usage Data (Optional): Call In Number, Call Out Number, Country Name, IP address, 911 Address (registered service address), Start and End time, Host Name, Host Email, MAC Address of device used

Special categories of data (if appropriate)

Special categories of data are not required to use the service. The data exporter may submit special categories of data to Customer, the extent of which is determined and controlled by the data exporter in its sole discretion. Such special categories of data include, but may not be limited to, Personal Data with information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sex life.

Processing operations

The personal data transferred may be subject to the following basic processing activities:

- account configuration and maintenance;
- facilitating conferences and meetings between data subjects and third party participants;

- hosting and storing personal data arising from such conferences and meetings solely for the purposes of providing the services;
- customer/ client technical and operational support.

DATA EXPORTER

Name: ………………………………………..…

Authorized Signature …………………………..

DATA IMPORTER

Name: Strigo Ltd.

Authorized Signature Amit Cohen

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

[Processor will implement and maintain the security measures set out in this Appendix 2 ("**Security Measures**"). Processor may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

Policies and Procedures

Processor will maintain policies and procedures designed to secure Personal Data processed on behalf of Controller against accidental or unlawful access or disclosure and identify and minimize reasonably foreseeable internal security risks, including the following:

Access Control

Access to Processor's facilities are granted to employees and contractors who have a legitimate business need for such access privileges.

Access to Strigo's Video and Web Conferencing Platform (the "**System**") requires a unique identification ("**ID**") to establish accountability with user logins.

Administrator access is restricted to authorized system and security administrators.

New user access to production is granted in accordance with the role matrix defined in the access control policy. Additional access requires management approval.

Access to critical systems and applications requires user IDs with passwords or public key authentication.

Physical access controls for data centers include key cards and biometric scanners, perimeter and interior IP-DVR, in-house staffing and mantrap and perimeter fencing.

Access reviews are performed quarterly for physical access to the collocated data centers.

Operations and System Integrity

Policy and procedures for processes, such as reporting operational failures, incidents, System problems, concerns, and user complaints (and the process for doing so), are made available to users

System capacity is reviewed periodically and action items are defined for capacity issues.

Data, transactions, and programs are backed up at a server level regularly. Production database systems are replicated across multiple regions.

Processor monitors a variety of communication channels for security incidents, and Strigo's security personnel will reach promptly to known incidents.

Processor performs and/or contracts with third-parties to perform vulnerability scans at least monthly and penetration testing annually.

Antivirus software is installed on workstations and laptops for users with access to production systems.

Processor has security policies that are approved by management at least annually.

Data transmission over customer portal is encrypted via Transport Layer Security ("**TLS**"). Access to the internal administrator tool is controlled via VPN.

Vendor systems are subject to review annually as part of the vendor risk management process, including reviewing independent third party reports.

Business continuity and disaster recovery plans, including restoration of backups, have been developed and are tested annually. The System is configured to provide failover capabilities to permit the resumption of critical operations.

Organization of Information and Personnel Security

Processor has formal organizational structures and defined roles. The security management plan and charter include an information security function and committee aligned within Processor, with defined structure and responsibilities.

Processor has defined job descriptions for personnel responsible for designing, developing, implementing, operating, monitoring, and maintaining the System.

Background or verification checks are performed on personnel (employees and contractors) when appropriate and permitted by local laws.

Personnel are required to read and accept the code of conduct and the statement of confidentiality during the onboarding process.

Trainings are conducted upon hire for all personnel.]