DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM (HEREINAFTER "DPA") RELATES TO THE PROCESSING OF PERSONAL DATA BY PGi IN ITS CAPACITY AS PROCESSOR IN THE COURSE OF PROVIDING THE SERVICES UNDER THE PGi SERVICES AGREEMENT AND THE RELEVANT GENERAL TERMS AND CONDITIONS (TOGETHER "**AGREEMENT**").

THIS DPA, WHICH HAS BEEN PRE-SIGNED BY PGi, IS BETWEEN (i) CUSTOMER AND/OR CUSTOMER AFFILIATE (TOGETHER "**CUSTOMER**") AND (ii) PGi, AND SHALL TAKE EFFECT AND BECOME BINDING UPON THE PARTIES WHEN PGi WILL RECEIVE THE COMPLETED AND SIGNED COPY BY CUSTOMER'S AUTHORISED SIGNATORY ON PAGE 5. FOR THE AVOIDANCE OF ANY DOUBT, THIS DPA SHALL NOT BE BINDING WHERE THE ENTITY SIGNING THIS DPA IS NOT A PARTY TO THE AGREEMENT, IS A CUSTOMER AFFILIATE NOT LEGALLY PERMITTED TO USE THE SERVICES OR IS AN END CUSTOMER THROUGH PGi AUTHORIZED RESELLER.

THIS DPA SHALL NOT REPLACE ANY COMPARABLE OR ADDITIONAL RIGHTS RELATING TO PROCESSING CONTAINED IN THE AGREEMENT.

PLEASE SUBMIT THE FULLY SIGNED COPY BY EMAIL TO **DPA@PGi.COM** INDICATING THE CUSTOMER ENTITY NAME IN THE SUBJECT MATTER. IF YOU HAVE CHOSEN TO EXECUTE THIS DPA THROUGH ADOBE SIGN, PLEASE FOLLOW THE INDICATIONS THAT YOU WILL RECEIVE AND E-SIGN.

DPA TERMS

PGi is Processing Personal Data as part of the performance of the Services contemplated in the Agreement. The purpose of this DPA is to set out the rights and obligations of the Parties in respect of the Personal Data Processed by PGi in its capacity as Processor under such Agreement.

1. Definitions

"Affiliates" means affiliates and subsidiaries, meaning a corporation or other entity of which a party owns, either directly or indirectly, more than fifty percent (50%) of the stock or other equity interests;
"Applicable Laws" means in respect of either Party, all laws, statutes, regulations, directions, guidelines and codes of conduct of any governmental or other regulatory body of competent jurisdiction, and any orders of any court or other tribunal of competent jurisdiction (together "**Laws**") which are applicable to the performance by that Party of its obligations or enjoyment of its rights under the Agreement and this DPA.
"Customer" / "You" means (i) the entity which is a party to this DPA and to the Agreement and (ii) where appropriate, that entity's EEA-based Affiliate which enters into this DPA;
"Data Protection Legislation" means European Regulation (EU) 2016/679 ("**GDPR**") and European Directive 2002/58/EC and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them, and all other Applicable Laws relating to Processing of Personal Data, privacy and communications secrecy that may exist in any relevant jurisdiction;
"Personal Data" means any information relating to an identified or identifiable natural person ('data subject') which information is subject to the GDPR or the laws of non-EU EEA countries that have formally adopted the GDPR and as interpreted in accordance with the GDPR;
"PGi" means the PGi entity which is a party to this DPA and to the Agreement with Customer, being: (i) American Teleconferencing Services Ltd. d/b/a as Premiere Global Services with address at 2300 Lakeview Parkway, Suite 300, Alpharetta, Georgia 30009 or, (ii) Premiere Conferencing (Ireland) Ltd with legal address at Unit E West Cork Technology Park, Clonakilty, Co. Cork Ireland;
"Agreement" means the PGi Services Agreement between PGi and the Customer for the provision of the Services and the General Terms and Conditions complementing the PGi Services Agreement entered into by the same Parties;
"**Privacy Shield**" means (i) for data transfers from the EEA (and the UK, at such time as the UK ceases to be a member state of the EU) to the U.S., the self-certification system by which U.S. organisations commit to a set of privacy principles issued by the U.S. Department of Commerce and approved by Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield; and (ii) for data transfers from Switzerland to the U.S., the self-certification system by

which U.S. organisations commit to a set of privacy principles issued by the U.S. Department of Commerce and approved by the Swiss Federal Data Protection and Information Commissioner.
"Services" means the PGi service offering provided by PGi to Customer under the Agreement;
"Standard Contractual Clauses" means the standard contractual clauses in the form adopted by Commission Decision 2010/87/EU 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 of the European Parliament and of the Council, executed by (i) Customer and (ii) American Teleconferencing Services Ltd. d/b/a as Premiere Global Services and appended to this DPA as Annex A.;
"Sub-processor" means any Processor engaged by PGi.

The terms "Controller", "Processor", "Process", "Processing", "Personal Data Breach", "Special Categories of Personal Data" and "Supervisory Authority" shall be interpreted in accordance with the GDPR.

2. Processor's obligations

2.1 The table below sets out the details of the Processing of Personal Data by PGi in its capacity as Processor:

Required details	Description
Subject-matter of Processing	Provision of the Services to the Customer in accordance with the Agreement.
Nature and purpose of Processing (Processing operations)	• Processing for the purposes of providing audio, video and web conferencing and webcasting services: retrieval, access, transmission, recording, storage and deletion. • Processing for the purposes of providing UCaaS services: transmission.
Categories of data subjects	• Subscribers to PGi services around the globe, Customer employees, agents or contractors; • Counterparties conducting video, web and/or audio conferences with the aforementioned data subjects; • Individuals identified in discussions, documents and electronic media disclosed during the use of the Services.
Types of Personal Data	• Business contact details (such as name, email-address, phone number, postal address), IP address; telephone access number; PIN code, the content of audio and video conference calls. It is not anticipated that Special Categories of Personal Data will be Processed by PGi.
Duration of Processing	For as long as PGi Processes Personal Data in its capacity as Processor under the Agreement.

2.2 PGi agrees that, in so far as Customer is the Controller for PGi's Processing activities, PGi shall:

2.2.1 Process Personal Data (and transfer Personal Data) only in accordance with Customer´s written instructions and in order to perform its obligations under the Agreement and not Process any Personal Data for any other purpose, unless required to do so by Applicable Laws to which PGi is subject; in such case, PGi will inform Customer of that legal requirement before Processing, unless that Law prohibits such information on important grounds of public interest. This DPA and the Agreement are Customer's complete and final instructions to PGi for the Processing of Personal Data under this DPA and, if applicable, the Standard Contractual Clauses. Any additional or alternate instructions must be agreed upon, and may be charged for, separately. The Customer accepts that the following all amount to instructions by the Customer to Process Personal Data: (a) Processing in accordance with the Agreement and applicable order form(s) or statement(s) of work; and (b) Processing initiated by users of the Services. PGi shall immediately inform the Customer if, in its opinion, an instruction from Customer infringes the GDPR or other European Union ("EU") or Member State data protection provision;

2.2.2 not disclose any Personal Data supplied by Customer to any other third party (other than as may be strictly necessary in the provision of the Services) without Customer´s prior written consent (such consent to not be unreasonably withheld or delayed), except where PGi is required by Applicable Laws to make such disclosure;

2.2.3 take all appropriate technological, physical and organisational measures to ensure a level of security of the Personal Data, appropriate to the risk, as those are set out in Annex B;

2.2.4 ensure that persons authorised to Process Personal Data have committed to confidentiality obligations or are under an appropriate statutory obligation of confidentiality;

2.2.5 notify the Customer, without undue delay, if PGi becomes aware of a Personal Data Breach and assist the Customer in meeting its obligations under articles 33 and 34 of the GDPR;

2.2.6 taking into account the nature of the Processing and the information available to PGi, assist the Customer in ensuring compliance with the Customer's obligations pursuant to articles 32 to 36 of the GDPR (to ensure a level of security of the Personal Data appropriate to the risk and, where applicable, to notify Personal Data Breaches to the Supervisory Authority/data subjects, to carry out data protection impact assessments and to consult the Supervisory Authority prior to Processing);

2.2.7 provide to the Customer reasonable assistance including by such technical and organisational measures, insofar as is possible, to comply with its obligations pursuant to articles 12 to 23 of the GDPR including any data subject access request;

2.2.8 provide the Customer, upon request, with any information and/or support which is necessary for the Customer to demonstrate that it has complied with its obligations under article 28 of the GDPR, including allowing for and contributing to audits or inspections carried out by the Customer and/or by a third party appointed by the Customer. The Parties agree that PGi will meet its obligations under this paragraph 2.2.8 and, where the Standard Contractual Clauses apply, under Clauses 5(f), 11 and 12(2) thereof, by using external independent security professionals selected by PGi to verify at least annually the adequacy of its security measures (the "Audit") and by providing to the Customer, upon Customer's request and subject to Customer undertaking confidentiality obligations, the result of such Audit in the form of a Systems and Organization Controls (SOC) 2 type II report on operational services ("Report"). In the event that the Customer wishes to undertake a different form of audit, the Customer may contact PGi in accordance with the "Notices" Section of the Agreement to request this. Before the commencement of any such alternative audit, Customer and PGi shall agree upon the costs, scope, timing, and duration of the audit, in addition to the reimbursement of the audit costs for the time spent by PGi. In the event that PGi and Customer fail to reach an agreement, Customer is entitled to terminate this DPA and the Agreement.

2.3 This paragraph 2.3 shall apply both to this DPA and, if the Standard Contractual Clauses apply, to the provisions in Clause 5(h) and 11 thereof. For the avoidance of doubt this paragraph 2.3 shall not apply in cases where PGi subcontracts ancillary services to third parties without having access to Personal Data; such ancillary services are not considered Processing.

2.3.1 Customer acknowledges and agrees that (a) PGi's Affiliates may be retained as Sub-processors; and (b) PGi may engage third-party Sub-processors in connection with the provision of the Services. PGi will make available to Customer a current list of Sub-processors engaged in connection with the provision of the Services with the identities of those Sub-processors upon request or by posting such list to PGi´s website at https://www.pgi.com/gdpr-subs/.

2.3.2 PGi shall be liable for the acts and omissions of its Sub-processors to the same extent as it would be liable if it performed the Processing carried out by each Sub-processor directly under the terms of this DPA.

2.3.3 PGi shall ensure that it imposes on any Sub-processor obligations equivalent to those imposed on it under this DPA and, if applicable, under the Standard Contractual Clauses.

2.3.4 PGi shall notify Customer if it wishes to change the list of Sub-processors. If Customer has reasonable grounds to object to PGi´s use of a new Sub-processor, Customer shall notify PGi promptly in writing within ten (10) business days from the date of notification. In the event that Customer objects and the objection is not unreasonable PGi will make reasonable efforts to make available to Customer a change in the Services affected or recommend a commercially reasonable change in the Services. If PGi is unable to make a reasonable change within sixty (60) days, Customer may terminate the Agreement, in respect of the affected Service which cannot be provided without the use of the objected Sub-processor, by prior notice in writing.

2.4 During the Term of the Agreement, Customer can, subject to limitations set out in Applicable Laws, access the Personal Data at any time and, subject to technical limitations, may export and retrieve such

Personal Data upon request or through the customer portal. On termination of this DPA, Customer hereby instructs PGi to delete the Personal Data Processed by PGi in its capacity as Processor within a reasonable period of time and in any event within 13 months of billing inactivity on a Customer account, unless PGi is required to retain such data for a further period in order to comply with Applicable Laws.

2.5 PGi will not independently respond to requests from Customer's end users without Customer's prior written consent, except where required by Applicable Laws.

3. Term

This DPA shall become effective when signed by both parties. Its duration shall depend on the duration of the Agreement. Termination of the Agreement shall therefore automatically result in termination of this DPA.

4. Limitation of liability

The Sections of the Agreement "Indemnity" and "Limitation of Liability" shall apply to the parties to this DPA and to the Standard Contractual Clauses and in such respect: (i) any references to Customer shall include Customer's Affiliates which are parties to this DPA, (ii) any references to PGi shall include the PGi entity entering into the Standard Contractual Clauses, and (iii) the term "Liability" shall have the meaning set out in the Agreement.

The total Liability, subject to the Agreement, of PGi (including that of PGi's Affiliates and suppliers) to Customer and Customer's Affiliates arising out of or in connection with this DPA or a breach of Data Protection Legislation, shall be limited to 12 months' Charges paid or payable for the Services during the year in which the Liability arises.

PGi does not intend to Process Special Categories of Personal Data on behalf of Customer and the Parties agree that no such data will be Processed under this DPA. If Customer submits or allows data subjects to submit such data, Customer acknowledges that it does so at its own risk and agrees to take responsibility for such Processing and shall indemnify and hold PGi and its Affiliates harmless against any costs, liability, damages, loss, claims or proceedings which may arise out of such Processing.

5. International data transfers outside the European Economic Area (the "EEA")

5.1 The terms in this Section 5 shall apply to the Processing of Personal Data by American Teleconferencing Services Ltd. (the "**Data Importer**") in the course of providing the Services.

5.2 Privacy Shield Certification

5.2.1 PGi confirms that the Processing of Personal Data transferred from the EEA, Switzerland, and the United Kingdom after it ceases to be a member state of the EU, to the Data Importer will be covered by the Data Importer's Privacy Shield certification, which the Data Importer will maintain throughout the Term of this DPA.

5.2.2 PGi will notify the Customer in writing in the event that (i) such certification ceases to be effective, is revoked or withdrawn, (ii) its status is otherwise challenged by a competent regulatory authority, or (iii) the Data Importer makes a determination that it can no longer meet its obligations under the Privacy Shield.

5.3 Application of the Standard Contractual Clauses

5.3.1 This Clause 5.3 and the Standard Contractual Clauses shall apply in the event that (i) Clause 5.2.1 ceases to be effective during the Term of this DPA or (ii) the Customer elects not to rely on the Data Importer's Privacy Shield certification, by stating so in the Agreement, The Standard Contractual Clauses shall apply to: (i) Customer and all Customer Affiliates that are located within the EEA, Switzerland and the UK after the UK has ceased to be a member state of the EU that have subscribed to the Services and which will be considered Data Exporters for the purposes of the Standard Contractual Clauses, and (ii) to American Teleconferencing Services Ltd., which will be considered Data Importer.

5.3.2 The Standard Contractual Clauses apply only to Personal Data that is transferred from the EEA, Switzerland and/or the UK after the UK has ceased to be a member state of the EU, to outside the UK, EEA and Switzerland as applicable, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an

adequate level of protection for personal data (as described in the GDPR) or, (ii) with regard to Personal Data transferred from Switzerland, as per Article 6(1) of the Swiss Federal Data Protection Act. Notwithstanding the foregoing, the Standard Contractual Clauses will not apply if PGi has adopted appropriate safeguards in light of article 46 of the GDPR or any of the conditions set forth in article 49 of the GDPR occur**.**

5.4 Switzerland

Where Personal Data is transferred from Switzerland outside of Switzerland, the definition of Personal Data shall under the Standard Contractual Clauses have the meaning assigned under the Swiss Federal Data Protection Act and, in accordance with Clause 9 of the Standard Contractual Clauses, the Data Exporter shall have the right to invoke the law of the EU or Swiss Customer Affiliate from which data originated (for EU and Swiss data, respectively).

5.5 Certification of Deletion

The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by the Data Importer to the Data Exporter only upon Data Exporter's request.

5.6 Conflict

The provisions in this DPA are intended to be clarifications as to how the parties will meet their obligations under the Standard Contractual Clauses. In the event that any of these provisions contradicts the Standard Contractual Clauses, then the Standard Contractual Clauses shall prevail to the extent of the contradiction.

6. Legal effect

This DPA is between Customer and, as applicable, the PGi entity which is a party to the Agreement and (save to the extent that this DPA and/or the Standard Contractual Clauses provide otherwise) is governed by the law specified in the Agreement and subject to the jurisdiction of the courts specified in that Agreement. In addition, American Teleconferencing Services Ltd, d/b/a Premiere Global Services is a party to the Standard Contractual Clauses in Annex A. Notwithstanding the signatures below of any other PGi entity, such other PGi entities are not a party to this DPA or the Standard Contractual Clauses.

In witness whereof, each of the undersigned companies have caused this DPA to be signed and delivered by its duly authorized representatives.

Customer Company Name

Authorized signature: _____

Name: _____

Title: _____

Date: _____

American Teleconferencing Services Ltd, d/b/a Premiere Global Services

Authorized signature: John Stone
John Stone (Sep 11, 2019)

Name: John Stone

Title: Chief Revenue Officer

Date: Sep 11, 2019

Premiere Conferencing (Ireland) Ltd.

Authorized signature: John Stone
John Stone (Sep 11, 2019)

Name: John Stone

Title: Chief Revenue Officer

Date: Sep 11, 2019

ANNEX A

STANDARD CONTRACTUAL CLAUSES

The Standard Contractual Clauses are available at the following link http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32010D0087 . The parties hereby agree that by reference to this link the Clauses shall be deemed incorporated into this DPA and made an integral part of it.

The parties to these Standard Contractual Clauses agree that the details required under Appendix 1 thereof are set out under paragraph 2.1 of the DPA to which these Standard Contractual Clauses are annexed and the security measures required under Appendix 2 to the Standard Contractual Clauses are those set out under paragraph 2.2.3 of such DPA. The parties further agree that paragraph 4 "Limitation of Liability" of such DPA shall apply to these Standard Contractual Clauses.

Customer company name

On behalf of the Data Exporter:

Name (written out in full):

Position:

Address:

Signature……

(stamp of organisation)

American Teleconferencing Services Ltd. d/b/a Premiere Global Services

On behalf of the Data Importer:

Name (written out in full): John Stone

Position: Chief Revenue Officer

Address: 17 Godliman Street, London

Signature John Stone John Stone (Sep 11, 2019) ……

(stamp of organisation)

ANNEX B - SECURITY MEASURES

1. Access control to premises and facilities

Measures must be taken to prevent unauthorized physical access to premises and facilities holding personal data. Measures shall include:

- Access control system
- ID reader, magnetic card, chip card or security guard
- (Issue of) keys
- Door locking (electric door openers etc.)
- Alarm system, for example video/CCTV monitor
- Logging of facility exits/entries

2. Access control to systems

Measures must be taken to prevent unauthorized access to IT systems. These must include the following technical and organizational measures for user identification and authentication:

- Password procedures (incl. special characters, minimum length, forced change of password)
- No access for guest users
- Management of system access
- Access to IT systems subject to approval from business management and IT system administrators

3. Access control to data

Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorised [input, reading, copying, removal] modification or disclosure of data. These measures shall include:

- Differentiated access rights by role
- Access rights defined according to duties
- Automated log of user access via IT systems
- Measures to prevent the use of automated data-processing systems by unauthorised persons using data communication equipment

4. Disclosure control

Measures must be taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure. These measures shall include:

- Encryption using a VPN or SSL/TLS for remote access, transport and communication of data.
- Prohibition of portable media

5. Input control

Measures must be put in place to ensure all data management and maintenance is logged.

Measures should include:

- Logging user activities on IT systems
- Ensure that it is possible to verify and establish which personal data have been input into automated data-processing systems and when the data were input;

6. Job control

Measures should be put in place to ensure that data is processed in compliance with the data importer's instructions. These measures must include:

- Unambiguous wording of contractual instructions
- Fulfilment of instructions by proper design of processes and procedures.

7. Availability control

Measures should be put in place to ensure that data are protected against accidental destruction or loss.

These measures must include:

- Ensuring that installed systems may, in the case of interruption, be restored
- Ensure systems are functioning, and that faults are reported
- Ensure stored personal data cannot be corrupted by means of a malfunctioning of the system
- Uninterruptible power supply (UPS)
- Business Continuity procedures
- Remote storage of backups of personal data
- Anti-virus/firewall systems

8. Segregation control

Measures should be put in place to allow data collected for different purposes to be processed separately.

These should include:

- Restriction of access to data stored for different purposes according to staff duties.
- Segregation of business IT systems
- Segregation of IT testing and production environments