



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 SERVICES AGREEMENT ENTERED INTO BETWEEN CUSTOMER AND PGI ("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 AND/OR CUSTOMER'S AFFILIATE AUTHORISED SIGNATORY ON PAGES 6 AND 7. 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 CONTRACTUALLY PERMITTED TO USE THE SERVICES OR IS AN END CUSTOMER THROUGH PGI AUTHORIZED RESELLER.

PLEASE SUBMIT THE FULLY SIGNED COPY BY EMAIL TO PRIVACY@PGI.COM INDICATING THE CUSTOMER ENTITY NAME IN THE SUBJECT MATTER.

DPA TERMS

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.

"California Consumer Privacy Act of 2018" or "**CCPA**" means Assembly Bill 375 of the California House of Representatives, an act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code;

"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, UK or Swiss Affiliate which enters into this DPA;

"Data Subject" means either (as applicable) (i) an identified or identifiable natural person whose rights are protected by the GDPR; or (ii) a "**Consumer**" as the term is defined in the CCPA;

"EEA" means European Economic Area;

"GDPR" means in each case to the extent applicable to the Processing: (i) Regulation (EU) 2016/679, as applicable from time to time; and (ii) Regulation (EU) 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland pursuant to and as amended by any legislation arising out of the withdrawal of the UK from the European Union;

"Personal Data" means any information that identifies a Data Subject which information is subject to the GDPR or CCPA or the laws of non-EU EEA countries that have formally adopted the GDPR and as interpreted in accordance with the GDPR or the CCPA;

"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 2475 Northwinds Pkwy, Suite 200 Alpharetta, GA 30009, United States (ii) TalkPoint Holdings LLC with address at 100 William Street 8th Floor New York, NY 10038 United States or, (ii) Premiere Conferencing (Ireland) Ltd with legal address at Unit E West Cork Technology Park, Clonakilty, Co. Cork Ireland;

"Agreement" means the services agreement between PGI and the Customer for the provision of the Services;

"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 Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council;

"Sub-processor" means any Processor engaged by PGI.

"Supervisory Authority" means as applicable: (i) a competent independent public authority responsible for monitoring the application of the GDPR or (ii) in respect of the CCPA, the California Attorney General and the California Privacy Protection Agency.

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



2. Processor's obligations

- a. 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)	<ul style="list-style-type: none"> • Processing for the purposes of providing online meetings with audio, video and screen sharing and/or solutions for hosting interactive webinars or large-scale webcast events. • Processing may include: use, retrieval, access, transmission by disclosure, recording, storage and deletion.
Categories of Data Subjects	<ul style="list-style-type: none"> • Customer employees, agents, contractors or, otherwise, participants to meetings and events; and • Data Subjects identified in recordings of meetings and events.
Types of Personal Data	<ul style="list-style-type: none"> • Host/moderator business contact details (such as name, email-address, phone number and postal address) and login credentials (username for webcast and PIN code and password for collaboration services); • Users : access number, IP address, email address or name; • Usage data: date and time of meeting or event, duration, connection quality, number of participants, web browser versions, bit rate to and from our servers; • The content recorded of meetings and events, transcriptions of such recording files, materials uploaded to the online platform for meetings and events and presenter and/or audience chat; and • Data facilitated for troubleshooting purposes or customer support (any of users and usage data above). <p>It is not anticipated that Special Categories of Personal Data will be Processed by PGI.</p>
Duration of Processing	For as long as PGI Processes Personal Data in its capacity as Processor under the Agreement, which unless otherwise agreed in the Agreement will be 13 months from the end of the provision of Services thereunder
Location of Processing	United States. Other countries where PGI has affiliates or Sub-processors would be involved where Controller requires support, maintenance or optional Services.
Recurrence of the transfer of Personal Data	This would depend on the type of Service and the frequency on which Controller requires support or uses the Services.

- b. PGI agrees that, in so far as Customer is the Controller for PGI's Processing activities, PGI shall:
- i. 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, if so agreed, order form(s) or statement(s) of work; and (b) Processing initiated by users of the Services (for example, when sending an invitation to participants by using the Services). PGI shall immediately inform the Customer if, in its opinion, an instruction from Customer infringes the GDPR, other European Union ("EU"), EU Member State or UK data protection provision;



- ii. not disclose any Personal Data supplied by Customer to any other third party 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;
 - iii. 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 and described under https://www.pgi.com/wp-content/uploads/2020/04/PGi-Security-Statement_Apr2020.pdf;
 - iv. ensure that persons authorised to Process Personal Data have committed to confidentiality obligations or are under an appropriate statutory obligation of confidentiality;
 - v. 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 (data breach reporting obligations);
 - vi. 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) and, where applicable, under CCPA (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);
 - vii. 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 and to respond to requests to exercise Data Subject rights under the CCPA ;
 - viii. 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 (obligations in relation to appointment of processors), 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 viii.2.b.viii 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"). Notwithstanding the aforementioned, in the event that the Customer wished 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.
- c. The following sub-paragraphs shall apply both to this DPA and, if the Standard Contractual Clauses apply, to the provisions in Clause 5(h) and 11 thereof.
- i. 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. The list of approved Sub-processors as of the effective date of this DPA is posted at PGI's website at <https://www.pgi.com/gdpr-subs/>.
 - ii. 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.
 - iii. PGI shall ensure that it imposes on any Sub-processor obligations no less onerous than those imposed on it under this DPA and, if applicable, under the Standard Contractual Clauses.
 - iv. PGI shall notify Customer if it wishes to change the list of Sub-processors via email, to Customer's preferred email address, which Customer shall provide to PGI by emailing: privacy@pgi.com. 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 an alternative Sub-processor or recommend a commercially reasonable change in the Services



that would not require the use of the Sub-processor. If PGI and Customer are unable to reach a solution within sixty (60) days from the date on which Customer objected, Customer will have the right to terminate the Agreement, if the Agreement cannot be performed without the use of the objected-to Sub-processor, by prior notice in writing.

- d. 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 Services platform. 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.
- e. PGI will not independently respond to requests from Data Subjects 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 addressing indemnification 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 in those sections shall include any 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 if different to the PGI entity which is a party to the Agreement, 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) to Customer and Customer's Affiliates arising out of or in connection with this DPA or a breach of Applicable Laws, shall be limited to 12 months' fees paid or payable for the Services during the year in which the liability arises.

Customer acknowledges that PGI does not require nor request the disclosure of Special Categories of Personal Data for the provision of the Services and PGI does not intend to Process Special Categories of Personal Data on behalf of Customer. If Customer submits or allows Data Subjects to submit such data, Customer acknowledges that it does so on its own responsibility and agrees to 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 EEA

- a. The terms in this Section 5 shall apply to the Processing of Personal Data by the PGI entity, American Teleconferencing Services Ltd. d/b/a Premiere Global Services or TalkPoint Holdings LLC, as the case may be (each, the "Data Importer"), in the course of providing the Services.

b. Application of the Standard Contractual Clauses

- i. PGI shall ensure that, where Personal Data is transferred by Premiere Conferencing (Ireland) Ltd from the EEA or Switzerland to a country that lacks a decision pursuant to art. 45 (3) of GDPR, a mechanism to adopt appropriate safeguards is in place, notably the Standard Contractual Clauses. The Standard Contractual Clauses shall apply between Data Importer and its Sub-Processors (Module 3 Processor to Processor Standard Contractual Clauses) available here https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc12-L_2021199EN.01003701-E0012. The parties hereby agree that by reference to this link these standard contractual clauses shall be deemed incorporated into this DPA and made an integral part..
- ii. Where transfers outside EEA or Switzerland are done by Customer or a Customer Affiliate to a Data Importer, then Standard Contractual Clauses Module 2 Controller to Processor



available here https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc12-L_2021199EN.01003701-E0012 shall apply and executed by Customer or the Customer Affiliate and the Data Importer. The parties hereby agree that by reference to this link these standard contractual clauses shall be deemed incorporated into this DPA and made an integral part.

- iii. Where transfers of Personal Data from the UK to outside the EEA or countries that have obtained an adequacy decision take place, the EU standard contractual clauses under 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 that are available at the following link <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32010D0087> (the “UK Standard Contractual Clauses”) will apply. The parties hereby agree that by reference to this link the UK Standard Contractual Clauses shall be deemed incorporated into this DPA and made an integral part.
- iv. The parties to the Standard Contractual Clauses and the UK Standard Contractual Clauses agree that the details required under Annex I and III of the Standard Contractual Clauses and under Appendix 1 of the UK Standard Contractual Clauses are set out under section 2 (a) and (c) i of this DPA and the security measures required under Annex II of the Standard Contractual Clauses and Appendix 2 to the UK Standard Contractual Clauses are those set out under Annex A of this DPA.

c. 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).

d. 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.

e. 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. CALIFORNIA CONSUMER PRIVACY ACT OF 2018

- a. PGi is a “Service Provider” as defined in CCPA Section 1798.140(v).
- b. Customer discloses Personal Data to PGi solely for: (i) a valid business purpose; and (ii) PGi to perform the Services.
- c. PGi is prohibited from: (i) selling Personal Data; (ii) retaining, using, or disclosing Personal Data for a commercial purpose other than providing the Services; and (iii) retaining, using, or disclosing the Personal Data other than as permitted by the Agreement.
- d. PGi understands and certifies that it will comply with the prohibitions outlined in Section 6.c.
- e. PGi may engage other Service Providers (as defined under the CCPA), to assist in providing the Services to Customer (“Sub-Service Providers”). PGi will ensure Sub-Service Providers comply with the CCPA and the provisions of this DPA, including certification by Sub-Service Providers that they understand the provisions and will comply with them.

7. 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 the event of any conflict or inconsistency between (i) the terms of this DPA (including the Standard Contractual Clauses) and (ii) the Agreement, the former shall prevail to the extent of the conflict or inconsistency.

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/ Controller/ Data Exporter

Authorized signature: _____
Name: _____
Title: _____
Date: _____

American Teleconferencing Services Ltd, d/b/a Premiere Global Services/ Processor/Data Importer

Authorized signature: *Michele Dobnikar*
MicheleDobnikar (Nov 25, 2021 05:38 MST)
Name: Michele Dobnikar
Title: President
Date: Nov 25, 2021

Premiere Conferencing (Ireland) Ltd./Processor

Authorized signature: *Michele Dobnikar*
MicheleDobnikar (Nov 25, 2021 05:38 MST)
Name: Michele Dobnikar
Title: President
Date: Nov 25, 2021

TalkPoint Holdings LLC/Processor/Data Importer

Authorized signature: *Michele Dobnikar*
MicheleDobnikar (Nov 25, 2021 05:38 MST)
Name: Michele Dobnikar
Title: President
Date: Nov 25, 2021

ANNEX A - 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 must 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 must 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