



THIS DATA PROCESSING ADDENDUM (HEREINAFTER "DPA") IS BETWEEN CUSTOMER OR CUSTOMER AFFILIATE AND PGI AND SHALL TAKE EFFECT AND BECOME BINDING BETWEEN PGI, CUSTOMER OR CUSTOMER AFFILIATES TO THE EXTENT THAT PGI OR ITS AFFILIATES PROCESSES CUSTOMER OR CUSTOMER AFFILIATES' PERSONAL DATA FOR WHICH THEY ARE DEEMED DATA CONTROLLERS, AND, WHERE THIS DPA IS REQUIRED UNDER THE APPLICABLE DATA PROTECTION LEGISLATION IN EACH CASE. FOR THE AVOIDANCE OF ANY DOUBT, THIS DPA SHALL NOT BE BINDING WHERE THE ENTITY SIGNING THIS DPA IS NOT A PARTY TO THE PGI SERVICES 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 PGI SERVICES AGREEMENT.

THIS DPA AND THE ATTACHED STANDARD CONTRACTUAL CLAUSES HAVE BEEN PRE-SIGNED BY PGI. WHEN PGI WILL RECEIVE THE COMPLETED AND SIGNED COPY BY CUSTOMER OR CUSTOMER AFFILIATE'S AUTHORIZED SIGNATORY ON PAGES 4, 6 AND 7, THIS DPA WILL BECOME A LEGALLY BINDING ADDENDUM TO THE PGI SERVICES AGREEMENT.

PLEASE SUBMIT THE FULLY SIGNED COPY BY EMAIL TO [DPA@PGi.COM](mailto: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

The data processor is receiving and processing personal data as part of the performance of the services contemplated in the PGI services agreement. The purpose of this DPA is to ensure the protection and security of personal data processed on behalf of data controller by data processor in accordance with the General Data Protection Regulation and applicable national data protection laws of the EU/EEA Member States.

### 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;

**"Customer" / "You"** means the entity which is a party to this DPA and to the PGI Services Agreement and that shall be deemed the Data Controller for purposes of this DPA;

**"Data Controller"** means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;

**"Data Processor"** means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the Data Controller;

**"Data Protection Legislation"** means the GDPR and all national laws and regulations of the European Union, European Economic Area, Switzerland and United Kingdom relating to the Processing of Personal Data;

**"GDPR"** means Regulation (EU) 2016/679;

**"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; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

**"PGi"** means the PGI entity which is a party to this DPA and to the PGI Services Agreement with Customer, being American Teleconferencing Services Ltd. d/b/a as Premiere Global Services with address at 2300 Lakeview Parkway, Suite 300, Alpharetta, Georgia 30009 or Premiere Conferencing (Ireland) Ltd with legal address at Unit E West Cork Technology Park, Clonakilty, Co. Cork Ireland, depending on the entity that is a party to the PGI Services Agreement, and that shall be deemed the Data Processor for purposes of this DPA;

**"PGi Services Agreement"** means the separate services agreement between the PGI entity and the Customer for the provision of conferencing services and collaboration solutions;

**"Processing"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, 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;

**"Services"** means the services provided by PGI under the PGI Services Agreement;



**“Standard Contractual Clauses”** means the agreement referenced in Annex A and approved by the European Commission for the transfer of Personal Data by data controllers to processors established outside of the European Economic Area executed between American Teleconferencing Services Ltd. d/b/a as Premiere Global Services and Customer or Customer Affiliate, as applicable;

**“Sub-processor”** means any Data Processor engaged by PGI or the PGI Affiliate hereunder.

## 2. Processing

2.1 Appendix 1 to this DPA sets out the details of the subject matter, nature and purpose of the data processing to be carried out by the Data Processor and the type of personal data and categories of data subjects. The duration of the processing will be for so long as PGI provides Services to Customer.

2.2 PGI agrees that, in so far as Customer is the Data Controller for PGI’s Data 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 PGI Services Agreement and not Process any Personal Data for any other purpose. This DPA and the PGI Services Agreement are Customer’s complete and final instructions to Data Importer for the Processing of Personal Data under the 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 PGI Services Agreement and applicable Order Form(s); 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 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 European Union or Member State law to make such disclosure, in which case PGI shall inform the Customer of that requirement before disclosure, unless PGI is prohibited by law, on important grounds of public interest, from notifying the Customer;

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 set out in Appendix 2;

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, once PGI becomes aware of a Personal Data breach and assist the Customer in meeting its obligations under articles 32 and 33 of the GDPR;

2.2.6 taking into account the nature of the processing and the information available to PGI, to assist the Customer in ensuring compliance with the Customer’s obligations pursuant to articles 32 and 34 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 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.

2.3 Customer agrees that PGI meets its obligations under 2.2.8 above and, where the Standard Contractual Clauses apply, under Clauses 5(f), 11 and 12(2) of the Standard Contractual Clauses (all referred to as "Audit") by making available to Customer information regarding PGI’s compliance with the obligations set forth in this DPA in the form of a report of a SOC 2 type II audit on operational services. 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 PGI Services Agreement to request this and Customer shall bear the entire costs of such Audit. Before the commencement of any such Audit, Customer and PGI shall agree upon the scope, timing, and duration of the Audit, in addition to the reimbursement of the Audit costs for the time spent by PGI, and reasonable confidentiality obligations for Customer and any third party appointed by Customer. Customer shall promptly notify PGI with information regarding any non-compliance discovered during the course of an Audit.



### **3. Sub-processors**

- 3.1 The following provisions in relation to Sub-processors apply both to the DPA and, if the Standard Contractual Clauses apply, to the provisions in Clause 5(h) and 11.
- 3.2 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.
- 3.3 For the avoidance of doubt this Section 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 Data Processing.
- 3.4 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 services of each Sub-processor directly under the terms of this DPA, unless otherwise set forth in the PGI Services Agreement.
- 3.5 PGI shall ensure that it imposes the same obligations on any Sub-processor as are imposed on it under this DPA and, if applicable, under the Standard Contractual Clauses.
- 3.6 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 PGI Services Agreement, in respect of the affected Service which cannot be provided without the use of the objected Sub-processor, by prior notice in writing.

### **4. Term**

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

### **5. Return and deletion of Customer data**

On termination of this DPA, Personal Data must be returned to Customer or deleted, at Customer's option. In no event shall PGI be required to return or delete data that (a) is retained for archival purposes which PGI shall delete in accordance with its usual policy for back-ups and that shall not be processed for any other purpose and subject to the security conditions herein, or (ii) is required to retain in order to comply with applicable European Union or Member State law (including a court order or regulatory order).

### **6. Right of data subjects**

PGI will not independently respond to requests from Customers' end users without Customer's prior written consent, except where required by applicable law.

### **7. Limitation of liability**

If American Teleconferencing Services d/b/a Premiere Global Services is not a party to the PGI Services Agreement, the Section of the PGI Services Agreement "Limitation of Liability" shall apply to American Teleconferencing Services Ltd d/b/a Premiere Global Services and in such respect any references to PGI shall include American Teleconferencing Services d/b/ Premiere Global Services.

If you submit any sensitive data or special categories of Personal Data, you do so at your own risk and you agree to take responsibility for consequences of your submission and you shall indemnify and hold harmless PGI against any costs, liability, damages, loss, claims or proceedings which may arise out of your failure to abide by this condition.



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

**8.1 Application of the Standard Contractual Clauses**

**8.1.1** The Standard Contractual Clauses and the terms in this Section shall apply to the Processing of Personal Data by American Teleconferencing Services Ltd. (the "Data Importer") in the course of providing the Services. The Standard Contractual Clauses shall apply to Customer and to all Customer Affiliates that are located within the EEA and Switzerland that have subscribed to the Services.

**8.1.2** The Standard Contractual Clauses apply only to Personal Data that is transferred from the European Economic Area (EEA) and/or Switzerland to outside the EEA and Switzerland, 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.

**8.2 Switzerland**

Where Personal Data is transferred from Switzerland outside of Switzerland, the definition of Personal Data shall 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 PGI Affiliate from which data originated (for EU and Swiss data, respectively).

**8.3 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.

**8.4 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.

**9. Legal effect**

This DPA is between Customer and, as applicable, the PGI entity which is a party to the PGI Services 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 PGI Services 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 as the Data Controller and Data Processor 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 (May 15, 2018)

---

Name: John Stone

---

Title: Chief Revenue Officer

---

Date: 15/05/2018

---

**Premiere Conferencing (Ireland) Ltd.**

Authorized signature: *John Stone*  
John Stone (May 15, 2018)

---

Name: John Stone

---

Title: Chief Revenue Officer

---

Date: May 15, 2018

---



**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.

**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: john.stone@pgi.com

Signature:   
John Stone (May 15, 2018)

(stamp of organisation)



## Appendix 1: DESCRIPTIONS OF DATA PROCESSING AND CATEGORIES OF DATA

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 the legal entity that is a party to these Clauses and that shall be deemed the data exporter and any Affiliates within the EEA and Switzerland that may disclose Personal Data to data importer as a consequence of the Services Agreement by and between the data importer and the data exporter.

### Data importer

The data importer is a service provider that provides audio conferencing services and collaboration solutions to data exporter hereunder.

### Data subjects

The personal data transferred concern the following categories of data subjects:

- Subscribers to PGi services around the globe, data exporter employees
- 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

### Categories of data

The personal data transferred concern the following categories of data: Name; email-address; IP-address; Telephone access number; PIN code, Identification numbers assigned to a data subject by the Data Importer; Video recordings; Photograph; Social media credentials or tokens; Other data processed as a result of Data Exporter and end users using the Services, including the content of audio and video conference calls.

### Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data: It is not anticipated that special categories of data are transferred to data importer or sub-processors

### Processing operations

The personal data transferred will be subject to the following basic processing activities): Retrieval, access, transmission, recording and storage in the course of providing support for Services

### DATA EXPORTER

Name: \_\_\_\_\_

Authorised Signature: \_\_\_\_\_

### DATA IMPORTER

Name: American Teleconferencing Services, Ltd. d/b/a Premiere Global Services

Authorised Signature: *John Stone*  
John Stone (May 15, 2018)



## Appendix 2: SECURITY MEASURES

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

### 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

### 1. 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

### 2. 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

### 3. 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

### 4. 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;





## **5. 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.

## **6. 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

## **7. 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