DATA PROCESSING ADDENDUM

This EU and UK Data Processing Addendum ("Addendum") supplements the Platform Service Agreement or similarly titled (the "Agreement") entered into by and between [Customer] ("Customer") and Globality, Inc. ("Company" or "Globality"), and any party which accedes to this Addendum from time to time pursuant to Clause 7 of the EU SCCs (as defined below). By executing the Addendum in accordance with Section 11 herein, Customer enters into this Addendum on behalf of itself and, to the extent required under applicable Data Protection Laws (defined below), in the name and on behalf of its Affiliates (defined below), if any. This Addendum incorporates the terms of the Agreement, and any terms not defined in this Addendum shall have the meaning set forth in the Agreement.

1. Definitions

1.1. "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2. "Authorized Sub-Processor" means a third-party who has a need to know or otherwise access Customer's Personal Data to enable Company to perform its obligations under this Addendum or the Agreement, and who is either (1) listed in Exhibit B or (2) subsequently authorized under Section 4.2 of this Addendum.

1.3. "Company Account Data" means personal data that relates to Company's relationship with Customer, including the names and email addresses of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account. Company Account Data also includes any data Company may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.

1.4. "Company Usage Data" means Service usage data collected and processed by Company in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

1.5. "Data Exporter" means Customer.

1.6. "Data Importer" means Company.

1.7. "Data Protection Laws" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data including: (i) the California Consumer Privacy Act ("CCPA"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR" or "GDPR"), (iii) the Swiss Federal Act on Data Protection, (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR"); (v) the UK Data Protection Act 2018; and (vi) the Privacy and Electronic Communications (EC Directive) Regulations 2003; in each case, as updated, amended or replaced from time to time. The terms "Data Subject", "Personal Data", "Personal Data Breach", "processing", "processor," "controller," and "supervisory authority" shall have the meanings set forth in the GDPR.

1.8. "EU SCCs" means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).

1.9. "ex-EEA Transfer" means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic Area (the "EEA"), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

1.10. "ex-UK Transfer" means the transfer of Personal Data, which is processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Exporter to the Data Importer (or its premises) outside the United Kingdom (the "UK"), and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

1.11. "Services" shall have the meaning set forth in the Agreement.

1.12. "Standard Contractual Clauses" means the EU SCCs and the UK SCCs.

1.13. "UK SCCs" means such standard data protection clauses as are adopted from time to time by the UK Information Commissioners Office ("ICO") in accordance with Article 46(2) of the UK GDPR including, but not limited to, the international data transfer agreement (UK IDTA), and the EU Standard Contractual Clauses as amended by ICO's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses.

2. Relationship of the Parties; Processing of Data

2.1. The parties acknowledge and agree that with regard to the processing of Personal Data, Customer may act either as a controller or processor and, except as expressly set forth in this Addendum or the Agreement, Company is a processor. Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Customer shall ensure that the processing of Personal Data in accordance with Customer's instructions will not cause Company to be in breach of the Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Company by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Company regarding the processing of such Personal Data. Customer shall not provide or make available to Company any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Company from all claims and losses in connection therewith.

2.2. Company shall not process Personal Data (i) for purposes other than those set forth in the Agreement and/or Attachment A, (ii) in a manner inconsistent with the terms and conditions set forth in this Addendum or any other documented instructions provided by Customer, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Supervisory Authority to which the Company is subject; in such a case, the Company shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest, or (iii) in violation of Data Protection Laws. Customer hereby instructs Company to process Personal Data in accordance with the foregoing and as part of any processing initiated by Customer in its use of the Services.

2.3. The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this Addendum.

2.4. Following completion of the Services, at Customer's choice, Company shall return or delete Customer's Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Company shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the UK SCCs and Clause 8.1(d) and Clause 8.5 of the EU SCCs (as applicable) shall be provided by Company to Customer only upon Customer's request.

2.5. CCPA. Except with respect to Company Account Data and Company Usage Data, the parties acknowledge and agree that Company is a service provider for the purposes of the CCPA (to the extent it applies) and is receiving personal information from Customer in order to provide the Services pursuant to the Agreement, which constitutes a business purpose. Company shall not sell any such personal information. Company shall not retain, use or disclose any personal information provided by Customer pursuant to the Agreement except as necessary for the specific purpose of performing the Services for Customer pursuant to the Agreement, or otherwise as set forth in the Agreement or as permitted by the CCPA. The terms "personal information," "service provider," "sale," and "sell" are as defined in Section 1798.140 of the CCPA. Company certifies that it understands the restrictions of this Section 2.5.

3. Confidentiality. Company shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Company's confidentiality obligations in the Agreement. Customer agrees that Company may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this Addendum, the Agreement, or the provision of Services to Customer

4. Authorized Sub-Processors

4.1. Customer acknowledges and agrees that Company may (1) engage its Affiliates and the Authorized Sub-Processors listed in Attachment B to this Addendum to access and process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of

providing the Services, including without limitation the processing of Personal Data. By way of this Addendum, Customer provides general written authorization to Company to engage sub-processors as necessary to perform the Services

4.2. A list of Company's current Authorized Sub-Processors (the "List") can be found at https://www.globality.com/globality-subprocessors. Such List may be updated by Company from time to time and Company may provide a mechanism to subscribe to notifications of new Authorized Sub-Processors and Customer agrees to subscribe to such notifications where available. At least fifteen (15) days before enabling any third party other than existing Authorized Sub-Processors to access or participate in the processing of Personal Data, Company will add such third party to the List and notify Customer via email. Customer may object to such an engagement by informing Company within ten (10) days of receipt of the aforementioned notice by Customer, provided such objection is in writing and based on reasonable grounds relating to data protection. Customer acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Company from offering the Services to Customer.

4.3. If Customer reasonably objects to an engagement in accordance with Section 4.2, and Company cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service by providing written notice to Company. Discontinuation shall not relieve Customer of any fees owed to Company under the Agreement.

4.4. If Customer does not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by Company, that third party will be deemed an Authorized Sub-Processor for the purposes of this Addendum.

4.5. Company will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Company under this Addendum with respect to the protection of Personal Data. In case an Authorized Sub-Processor fails to fulfill its data protection obligations under such written agreement with Company, Company will remain liable to Customer for the performance of the Authorized Sub-Processor's obligations under such agreement.

4.6. If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Company of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Company to Customer pursuant to Clause 5(j) of the UK SCCs or Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by the Company beforehand, and that such copies will be provided by the Company only upon request by Customer.

5. Security of Personal Data. 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, Company shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data. Attachment C sets forth additional information about Company's technical and organizational security measures.

6. Transfers of Personal Data.

6.1. The parties agree that Company may transfer Personal Data processed under this Addendum outside the EEA, the UK, or Switzerland as necessary to provide the Services. Customer acknowledges that Company's primary processing operations take place in the United States, and that the transfer of Customer's Personal Data to the United States is necessary for the provision of the Services to Customer. If Company transfers Personal Data protected under this Addendum to a jurisdiction for which the European Commission has not issued an adequacy decision, Company will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

6.2. Ex-EEA Transfers. The parties agree that ex-EEA Transfers are made pursuant to the EU SCCs, which are deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

6.2.1. Module One (Controller to Controller) of the EU SCCs apply when Company is processing Personal Data as a controller pursuant to Section 9 of this Addendum.

6.2.2. Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Company is processing Personal Data for Customer as a processor pursuant to Section 2 of this Addendum.

6.2.3. Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and Company is processing Personal Data on behalf of Customer as a sub-processor.

6.2.4. Module Four (Processor to Controller) of the EU SCCs apply when Customer is a processor of Company Usage Data and Company processes Company Usage Data as a controller.

6.3. For each module, where applicable the following applies:

6.3.1. The optional docking clause in Clause 7 does apply;

6.3.2. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 4.2 of this Addendum;

6.3.3. In Clause 11, the optional language does not apply;

6.3.4. All square brackets in Clause 13 are hereby removed;

6.3.5. In Clause 17 (Option 1), the EU SCCs will be governed by Republic of Ireland law;

6.3.6. In Clause 18(b), disputes will be resolved before the courts of Republic of Ireland;

6.3.7. Attachment B to this Addendum contains the information required in Annex I of the EU SCCs;

6.3.8. Attachment C to this Addendum contains the information required in Annex II of the EU SCCs; and

6.3.9. By entering into this Addendum, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

6.4. Ex-UK Transfers. The parties agree that ex-UK Transfers are made pursuant to the UK SCCs, which are deemed entered into and incorporated into this Addendum by reference, and completed as follows:

6.4.1. References to the GDPR will be deemed to be references to the UK GDPR and the UK Data Protection Act 2018, references to "supervisory authorities" will be deemed to be references to the UK Information Commissioner, and references to "Member State(s)" or the EU will be deemed to be references to the UK.

6.4.2. The UK Controller-to-Processor SCCs apply when the Company processes Customer's Personal Data as a processor. The illustrative indemnification clause does not apply. In Clause 4(f) the language "adequate protection within the meaning of Directive 95/46/EC" is deleted and replaced with "a level of data protection that is considered adequate under, or equivalent to, the applicable data protection law." Clause 9, Governing Law, shall read "The Clauses shall be governed by the law of the Member State in which the data exporter is established, but without prejudice to the rights and freedoms that data subjects may enjoy under their national data protection laws." In Clause 11(3), the language ", namely..." at the end of the sentence is hereby deleted. Attachment B of this Addendum serves as Appendix I of the UK Controller-to-Processor SCCs. Attachment C of this Addendum serves as Appendix II of the UK Controller-to-Processor SCCs.

6.4.3. The UK Controller-to-Controller SCCs apply when the Company processes Customer's Personal Data as a controller pursuant to Section 9 of this Addendum. Clause II(h) of the UK Controller-to-Controller SCCs shall be deemed to state that the Company will process Personal Data in accordance with the data processing principles set forth in Annex A of the UK Controller-to-Controller SCCs. The illustrative commercial clause does not apply. Clause IV (Governing Law) shall read "The Clauses shall be governed by the law of the Member State in which the data exporter is established, but without prejudice to the rights and freedoms that data subjects may enjoy under their national data protection laws." Attachment B of this Addendum serves as Annex B of the UK Controller-to-Controller SCCs.

6.4.4. The parties acknowledge and agree that if any of the UK SCCs are replaced or superseded by new standard contractual clauses issued and approved pursuant to Article 46 of the UK GDPR and related provisions of the UK Data Protection Act 2018 ("New UK SCCs"), the Data Importer may give notice to the Data Exporter and, with effect from the date set forth in such notice, the

application of the UK SCCs set forth in this Addendum shall be amended so that the UK SCCs cease to apply to ex-UK Transfers, and the New UK SCCs specified in such notice shall apply going forward. To the extent that the use of the New UK SCCs require the parties to complete additional information, the parties shall reasonably and promptly work together to complete such additional information.

6.5. Transfers from Switzerland. The parties agree that transfers from Switzerland are made pursuant to the EU SCCs with the following modifications:

6.5.1. The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the "FADP," and as revised as of 25 September 2020, the "Revised FADP") with respect to data transfers subject to the FADP.

6.5.2. The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

6.5.3. Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner ("FDPIC") of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Section 13 shall be observed.

6.5.4. The term "EU Member State" as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

6.6. Supplementary Measures. In respect of any ex-EEA Transfer or ex-UK Transfer, the following supplementary measures shall apply:

6.6.1. As of the date of this Addendum, the Data Importer has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) Customer's Personal Data ("Government Agency Requests");

6.6.2. If, after the date of this Addendum, the Data Importer receives any Government Agency Requests, Company shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort, Company may provide Customer's basic contact information to the government agency. If compelled to disclose Customer's Personal Data to a law enforcement or government agency, Company shall give Customer reasonable notice of the demand and cooperate to allow Customer to seek a protective order or other appropriate remedy unless Company is legally prohibited from doing so. Company shall not voluntarily disclose Personal Data to any law enforcement or government agency. Data Exporter and Data Importer shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this Addendum should be suspended in the light of the such Government Agency Requests; and

6.6.3. The Data Exporter and Data Importer will meet regularly to consider whether:

6.6.3.1. the protection afforded by the laws of the country of the Data Importer to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, whichever the case may be;

6.6.3.2. additional measures are reasonably necessary to enable the transfer to be compliant with the Data Protection Laws; and

6.6.3.3. it is still appropriate for Personal Data to be transferred to the relevant Data Importer, taking into account all relevant information available to the parties, together with guidance provided by the supervisory authorities.

6.6.4. If Data Protection Laws require the Data Exporter to execute the Standard Contractual Clauses applicable to a particular transfer of Personal Data to a Data Importer as a separate agreement, the Data Importer shall, on request of the Data Exporter, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Data Exporter to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant Data Protection Laws.

6.6.5. If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA or UK set forth in this Addendum cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Data Importer may by notice to the Data Exporter, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Protection Laws.

7. Rights of Data Subjects.

7.1. Company shall, to the extent permitted by law, notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of processing, withdrawal of consent to processing, and/or objection to being subject to processing that constitutes automated decision-making (such requests individually and collectively "Data Subject Request(s)"). If Company receives a Data Subject Request in relation to Customer's data, Company will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Company, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

7.2. Company shall, at the request of the Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, provided that (i) Customer is itself unable to respond without Company's assistance and (ii) Company is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8. Actions and Access Requests; Audits

8.1. Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, provided that Customer does not otherwise have access to the relevant information. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8.2. Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8.3. Company shall maintain records sufficient to demonstrate its compliance with its obligations under this Addendum, and retain such records for a period of three (3) years after the termination of the Agreement. Customer shall, with reasonable notice to Company, have the right to review, audit and copy such records at Company's offices during regular business hours.

8.4. Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Company shall, either (i) make available for Customer's review copies of certifications or reports demonstrating Company's compliance with prevailing data security standards applicable to the processing of Customer's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Customer's independent third party representative to conduct an audit or inspection of Company's data security infrastructure and procedures that is sufficient to demonstrate Company's compliance with its obligations under Data Protection Laws, provided that (a) Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Company's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to Customer. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Company for any time expended for on-site audits. If Customer and Company have entered into Standard Contractual Clauses as

described in Section 6 (Transfers of Personal Data), the parties agree that the audits described in Clause 5(f) and Clause 12(2) of the UK SCCs and Clause 8.9 of the EU SCCs shall be carried out in accordance with this Section 8.4.

8.5. Company shall immediately notify Customer if an instruction, in the Company's opinion, infringes the Data Protection Laws or Supervisory Authority.

8.6. In the event of a Personal Data Breach, Company shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as Company in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Company's reasonable control).

8.7. In the event of a Personal Data Breach, Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

8.8. The obligations described in Sections 8.6 and 8.7 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Company's obligation to report or respond to a Personal Data Breach under Sections 8.6 and 8.7 will not be construed as an acknowledgement by Company of any fault or liability with respect to the Personal Data Breach.

9. **Company's Role as a Controller.** The parties acknowledge and agree that with respect to Company Account Data and Company Usage Data, Company is an independent controller, not a joint controller with Customer. Company will process Company Account Data and Company Usage Data as a controller (i) to manage the relationship with Customer; (ii) to carry out Company's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Customer; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Company is subject; and (vi) as otherwise permitted under Data Protection Laws and in accordance with this Addendum and the Agreement. Company may also process Company Usage Data as a controller to provide, optimize, and maintain the Services, to the extent permitted by Data Protection Laws. Any processing by the Company as a controller shall be in accordance with the Company's privacy policy set forth at https://www.globality.com/privacy-and-cookie-policy.

10. **Conflict.** In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this Addendum; (3) the Agreement; and (4) the Company's privacy policy. Any claims brought in connection with this Addendum will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

Customer	**Globality, Inc.**
Signature:_____	Signature:_____
Print Name:_____	Print Name:_____
Title:_____	Title:_____

Date:_____	Date:_____

Attachment A

Details of Processing

Nature and Purpose of Processing

Globality will Process Personal Data as necessary to perform the Services pursuant to the Agreement, and as further instructed by Customer in its use of the Services.

Duration of Processing

Company will process Customer's Personal Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Company's legitimate business needs; or (iii) by applicable law or regulation. Company Account Data and Company Usage Data will be processed and stored as set forth in Company's privacy policy.

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's Users authorized by Customer to use the Services

Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Customer's registration data (e.g., name, email address, account password);
- Information regarding User activities on Customer's platform (such as frequency of activity, subscription status, etc.)

Special categories of data (if appropriate)

None

Attachment B

The following includes the information required by Annex I and Annex III of the EU SCCs, and Appendix 1 of the UK SCCs.

1. **The Parties**

Data exporter(s):
Name: [Customer]

Address:

Contact person's name, position and contact details: as provided in the Agreement

Activities relevant to the data transferred under these Clauses:

Signature and date:

Role (controller/processor): Controller

Data importer(s):

Name: Globality, Inc.

Address: 395 Page Mill Rd. Palo Alto CA 94306

Contact person's name, position and contact details: Chief Privacy Officer privacy@globality.com

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): Processor

Accession Form (if needed)

Additional parties added pursuant to Clause 7 of the EU SCCs:

Data exporter(s):
Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and accession date:

Role (controller/processor):

Data importer(s):

Name: …

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and accession date: …

Role (controller/processor):

2. Description of the Transfer

Data Subjects	As described in Exhibit A of the Addendum
Categories of Personal Data	Customer employees and/or customer provider employees: - First and Last Name - Email Address - IP Address Profile Image (optional)
Special Category Personal Data (if applicable)	Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion
Nature of the Processing	As described in Exhibit A of the Addendum
Purposes of Processing	As described in Exhibit A of the Addendum
Duration of Processing and Retention (or the criteria to determine such period)	As described in Exhibit A of the Addendum
Frequency of the transfer	As necessary to provide perform all obligations and rights with respect to Personal Data as provided in the Agreement or Addendum
Recipients of Personal Data Transferred to the Data Importer	Company will maintain and provide a list of its Subprocessors upon request.

3. Competent Supervisory Authority

The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13.

4. List of Authorized Sub-Processors

https://www.globality.com/globality-subprocessors contains an up-to-date list of the subprocessors utilized to provide the Services.

Attachment C

Description of the Technical and Organisational Security Measures implemented by the Data Importer

The following includes the information required by Annex II of the EU SCCs and Appendix 2 of the UK SCCs.

Technical and Organizational Security Measure	Details
Measures of pseudonymization and encryption of personal data	All customer data is treated with the utmost confidentiality and sensitivity and is encrypted at rest and in transit with industry strength encryption algorithms. Personal information used for AI modeling is thoroughly sanitized and de-identified both programmatically and manually before it is used internally.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Globality uses autoscaling servers to ensure availability of platform resources. Platform capacity is continuously monitored and tweaked to ensure high availability.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Globality regularly backs up customer data as well as continuously replicates data to a separate disaster recovery region. This ensures that in the case of a disaster, customer data and platform functionality can be quickly restored.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Globality conducts annual comprehensive external penetration tests as well as ISO 27001 and SOC 2 Type 2 audits.
Measures for user identification and authorization	Globality provides customers the ability to integrate with their IdP via SAMLv2.0 for SSO functionality. In the case that SSO is not used, Globality provides stringent password requirements and MFA.
Measures for the protection of data during transmission	All customer data is encrypted in transit via TLSv1.2
Measures for the protection of data during storage	All customer data is encrypted at rest via AES 256
Measures for ensuring physical security of locations at which personal data are processed	Globality is entirely cloud native and does not store customer data at any physical Globality location.
Measures for ensuring events logging	All platform events and/or user activities are logged and monitored. This includes information such as timestamps, non-sensitive user IDs, affected service(s), action performed, and more.
Measures for ensuring system configuration, including default configuration	Globality's platform is highly configurable to ensure it can meet customer requirements.
Measures for internal IT and IT security governance and management	Globality has a dedicated Information Security team that is responsible for overseeing, managing, monitoring, and auditing Globality's security posture. Globality's InfoSec organization is ISO 27001 certified.

Measures for certification/assurance of processes and products	Globality is ISO 27001 and SOC 2 Type 2 certified.
Measures for ensuring data minimisation	Globality only collects, stores, and processes the minimum amount of data required to provide platform services.
Measures for ensuring data quality	Globality collects data directly from customers and end users. While this information is sanitized before processing, Globality uses what information customers provide.
Measures for ensuring limited data retention	Globality will return and/or delete customer data upon request.
Measures for ensuring accountability	All Globality staff must go through annual security and privacy training – including attestations to our company policies. All staff undergo background checks prior to employment and must sign an NDA before starting.
Measures for allowing data portability and ensuring erasure	Globality is GDPR compliant and provides customers the rights to data portability and/or erasure.
Technical and organizational measures of sub-processors	Globality vets all sub processors prior to onboarding to ensure they have proper security and privacy controls. A DPA is also signed with any sub processor before they can handle customer personal information.

Globality will, as a minimum, implement the following types of security measures with respect to the Services:

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, include:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system;
- Securing decentralized data processing equipment and personal computers.

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of one master record per user, user master data procedures, per data processing environment;
- Encryption of archived data media.

3. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access personal data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure;
- Encryption.

4. Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- Encryption/Tunneling;
- Logging;
- Transport security.

5. Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems;
- Audit trails and documentation.

6. Control of instructions

Technical and organizational measures to ensure that Personal Data are processed solely in accordance with the instructions of Subscriber include:

- Unambiguous wording of the contract;
- Formal commissioning (request form);
- Criteria for selecting the Processor.

7. Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems;
- Disaster recovery plan.

8. Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately include:

- Separation of databases;
- “Internal client” concept / limitation of use;
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes.