Globalgig
Data Processing Addendum

This Data Processing Addendum is updated to reflect 2025–2026 global standards, including GDPR, updated SCCs, EDPB guidance, international transfer requirements, TIA obligations, and global model clause convergence.

GLOBALGIG DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM ("**DPA**" or "**Addendum**"), forms part of the Main Services Agreement or similar agreement and together with any related Service Addenda, Service Order, and Globalgig Policy, as may be amended from time to time (collectively, the "**Agreement**"), is effective immediately ("**Effective Date**"),

BY and BETWEEN:

1. the Globalgig Entity identified in the Agreement, including any applicable Service Order ("**Globalgig**" or "**Company**"); and
2. the customer identified in the Agreement, including any applicable Service Order, or within Globalgig's billing systems, or as a User of a Globalgig Service ("**Customer**"),

each referred to individually as a "**Party**" and together as the "**Parties**".

WHEREAS:

1. Globalgig offers to provide products and services under the terms outlined in its Agreement ("**Service(s)**"); and
2. Customer agrees to provide payment and other considerations, which constitute a valid and sufficient consideration to support the formation of a binding contract; and
3. By accessing or using Services, Customer agrees to be bound by this Addendum.
4. Continued use of a Service constitutes acceptance of this Addendum and the Agreement.
5. Both Parties acknowledge that this exchange of promises and obligations represents mutual consideration, and that in consideration of the mutual covenants contained in this Addendum and for other good and valuable consideration, the receipt of which is hereby acknowledged, and intending to be legally bound, the Parties agree as follows:

AGREED TERMS:

1. Subject Matter and Duration

a) **Subject Matter.** This Addendum reflects the Parties' commitment to abide by Applicable Data Protection Laws concerning the Processing of Customer Personal Data in connection with Company's execution of the Agreement. All capitalized terms that are not expressly defined in this DPA will have the meanings given to them in the Agreement. If and to the extent language in this Addendum or any of its Exhibit's conflict with the Agreement, this Addendum shall control.

b) **Duration and Survival.** Company will Process Customer Personal Data until the relationship terminates as specified in the Agreement. Company's obligations and Customer's rights under this Addendum will continue in effect so long as Company Processes Customer Personal Data.

2. Definitions

"**Applicable Data Protection Laws**" means all data protection and privacy laws applicable to the Processing of Customer Personal Data, including, as applicable, the EU/EEA GDPR, the UK GDPR and the Data Protection Act 2018, the Swiss FADP, Brazil's LGPD, Canada's PIPEDA, the California Consumer Privacy Act as amended by the CPRA, and other U.S. state privacy laws, together with their implementing regulations and binding guidance.

"**Customer Personal Data**" means Personal Data pertaining to Customer's Data Subjects that Company Processes to provide the Services, as further described in Exhibit 1.

"**Controller**", "**Processor**", "**Personal Data**", "**Personal Data Breach/Security Incident**", "**Process/Processing**", and "**Sub-processor**" have the meanings given in Applicable Data Protection Laws.

"**Globalgig Entity**" includes IGEM COMMUNICATIONS LLC (DBA Globalgig), a Texas limited liability company, and its Affiliates, with a principal place of business at 1870 W. Bitters Road, Suite 103, San Antonio, Texas 78248, and GLOBALGIG LIMITED, a company incorporated under the laws of England and Wales (registered no 08164402), having its registered office at 1 Quality Court, Chancery Lane, London WC2A 1HR.

"**SCCs**" means the European Commission's standard contractual clauses, including the 2021 modernised SCCs and any additional SCCs adopted by the Commission to address transfers to importers directly subject to the GDPR, together with the UK International Data Transfer Agreement or Addendum, and the Swiss FDPIC-aligned clauses, as applicable.

"**International Transfer**" means a transfer of Personal Data to a country outside the applicable jurisdiction (EU/EEA/UK/Switzerland) or to an international organisation.

3. Roles and Scope

3.1 Roles. Customer is Controller and Company is Processor with respect to Customer Personal Data. Where Company engages Sub-processors, Company acts as a Processor engaging Sub-processors on behalf of Customer under GDPR as applicable.

3.2 Documented Instructions. Company shall Process Customer Personal Data only on documented instructions from Customer, including regarding International Transfers. If an instruction infringes Applicable Data Protection Laws, Company shall promptly notify Customer.

4. Purpose Limitation and Use Restrictions

4.1 Purpose Limitation. Company shall Process Customer Personal Data solely to provide the Services and as documented by Customer. Company shall not "sell" or "share" Customer Personal Data as defined by CPRA or use it for cross-context behavioral advertising.

4.2 Confidentiality. Company shall ensure persons authorized to Process Customer Personal Data are bound by confidentiality obligations.

5. Security

5.1 Security Program. Company shall implement and maintain an Information Security Program aligned with recognized standards (e.g., ISO/IEC 27001/27002), including: encryption in transit and at rest with secure key management; least-privilege access and multi-factor authentication; network segmentation and continuous monitoring; vulnerability management and at least annual penetration testing; secure software development lifecycle (SSDLC); and tested incident response, business continuity, and disaster recovery plans.

5.2 Personnel and Access. Company shall limit access to Customer Personal Data to authorized personnel with a need-to-know and maintain role-based access controls.

6. Security Incidents

6.1 Notice. Company shall notify Customer without undue delay and, where GDPR applies, in any event within forty-eight (48) hours after becoming aware of a Security Incident affecting Customer Personal Data, providing available details and rolling updates until containment.

6.2 Cooperation. Company shall investigate, mitigate, and remedy Security Incidents and cooperate with Customer on notifications to authorities or Data Subjects as required by law.

7. Sub-processors

7.1 Authorization. Customer authorizes Company to engage Sub-processors necessary to provide the Services, subject to this Section 7 (SUB-PROCESSORS).

7.2 Flow-down. Company shall impose data protection obligations on Sub-processors no less protective than this DPA.

7.3 Changes. Company shall provide advance notice of new or replacement Sub-processors and allow Customer thirty (30) days to object on reasonable grounds. The Parties will work in good faith negotiations to resolve said objection.

8. International Data Transfers

8.1 Current Data Residency. Based on the Services provided to Customer; Company does not perform International Transfers of Customer Personal Data. Customer agrees that Sections 8.2–8.6 apply only if and to the extent an International Transfer occurs.

8.2 Transfer Mechanisms. Company shall not perform an International Transfer unless it has implemented: (a) an adequacy decision (e.g., EU-US Data Privacy Framework/Swiss-US/UK Extension, where applicable to the recipient); (b) SCCs (including the 2021 SCCs, Module Two, and any additional SCCs adopted by the European Commission for importers subject to GDPR); (c) Binding Corporate Rules; or (d) another lawful mechanism under Chapter V GDPR/UK GDPR/FADP.

8.3 SCC Details (EU/EEA). Where SCCs are used: Customer is the data exporter and Company the data importer; Annex I details are in Exhibit 1; Annex II measures are in Exhibit 2; Clause 9: Option 2 with the notice period in Section 6.3; Clause 11: not used; Clause 17: law of Ireland; Clause 18(b): courts of Ireland.

8.4 UK Transfers. For UK transfers, the UK IDTA or UK Addendum to the EU SCCs is incorporated with Parties' details and Key Contacts as in Exhibit 1; the Approved EU SCCs are the 2021 SCCs; annexes per Exhibit 1 and Exhibit 2; termination per the IDTA/Addendum.

8.5 Swiss Transfers. For Swiss transfers, the 2021 SCCs apply with FADP modifications including FDPIC as authority and Swiss forum rights for Data Subjects; where both GDPR and FADP apply, dual supervisory competence is recognized.

8.6 TIAs and Supplementary Measures. Company shall cooperate with Customer to complete Transfer Impact Assessments ("**TIA(s)**") and implement supplementary measures (e.g., encryption and key management) as reasonably required.

9. Government Authority Requests

9.1 Notices. Unless legally prohibited, Company shall promptly notify Customer of any request from a public authority for access to Customer Personal Data.

9.2 Challenge and Minimization. Company shall work in good faith to challenge unlawful or overbroad requests and disclose only the minimum data required by law, documenting the assessment and outcome.

10. Data Subject Requests

10.1 Assistance. Taking into account the nature of Processing, Company shall work in good faith to assist Customer by appropriate technical and organizational measures to fulfil Data Subject requests under Applicable Data Protection Laws and shall not respond directly unless authorized or required by law.

11. Audits and Information

11.1 Information. Company shall make available to Customer information necessary to demonstrate compliance with this DPA and applicable SCCs.

11.2 Audit. Customer (or its independent auditor) may audit Company's relevant policies, controls, and facilities: (i) after a Security Incident; (ii) upon reasonable belief of non-compliance; (iii) when required by a regulator; or (iv) once per 12 months with reasonable notice, scope, and timing; third-party auditors must be bound by confidentiality. Where material non-compliance is found, Company shall remediate promptly.

12. Return and Deletion

12.1 Upon termination or upon Customer's written instruction, Company shall return a copy of Customer Personal Data (if requested) and securely delete all Customer Personal Data. Where data is retained in backups, such data shall be securely isolated, protected from further processing, and deleted in accordance with Company's backup retention schedule, unless legally required to be retained, and certify deletion upon request.

13. Assistance; DPIAs; Records

13.1 Company shall provide reasonable assistance for Data Protection Impact Assessment ("**DPIA(s)**") and, where required, prior consultation with supervisory authorities. Company shall maintain records of Processing as required by Applicable Data Protection Laws.

14. Liability and Indemnity

14.1 Company's liability and Customer's remedies under this DPA are subject to the limitations and exclusions in the Agreement; provided, that, in absence of limitations and exclusions, Customer agrees that the entire liability of Company arising under or in connection with this DPA, and however arising, whether in contract, tort (including negligence or breach of statutory duty), misrepresentation or otherwise, and whether or not Company was aware of the possibility of such loss arising, shall be limited to the total amount paid by Customer under the Agreement. Company shall indemnify Customer against third-party Claims to the extent arising from Company's gross negligence or wilful breach of this DPA or Applicable Data Protection Laws, except to the extent caused by or resulting from Customer or other third party or events outside of the reasonable control of Company.

15. Order of Precedence; Changes in Law

15.1 In case of conflict between this DPA and the Agreement, this DPA controls to the extent of the conflict. In case of conflict between this DPA and the SCCs, the SCCs prevail.

15.2 If changes in law or regulator guidance require updates (including additional SCCs adopted by the European Commission for GDPR-subject importers), the Parties shall in good faith execute necessary documents to maintain compliance.

16. Miscellaneous

16.1 Governing law, dispute resolution, and notices follow the Agreement, except as required by applicable transfer mechanisms.

17. Acceptance of this Addendum

17.1 USE OF A SERVICE CONSTITUTES ACCEPTANCE OF THIS ADDENDUM BY CUSTOMER.

17.2 This Addendum constitutes a final agreement between the Parties and supersedes all prior agreements relating to the subject matter hereof, which are of no further force or effect.

17.3 Any and all Services pertaining to the subject matter hereof and active as of the Effective Date shall be governed by this Addendum.

17.4 There are no oral agreements between the Parties.

17.5 No Party is entering into this Addendum in reliance on, and this Addendum shall not be contradicted or supplemented by, any prior or contemporaneous:

17.5.1 condition, discussion, promise, statement, understanding, or undertaking;

17.5.2 letter of intent, memorandum of understanding, commitment, or approval; and/or

17.5.3 other agreements, such as pre-printed forms, purchase orders, acknowledgments, or security or specification forms, which are for convenience purposes only, and all terms and conditions stated thereon are void and of no effect under this Agreement.

17.5.4 This Addendum may be amended only by written notice by Globalgig, except where amendments are required to comply with Applicable Data Protection Laws.

[END OF DPA MAIN BODY]

[EXHIBITS 1 – 3 ON FOLLOWING PAGES]

Exhibit 1 — Details of Processing

A. Subject Matter: Provision of the Services under the Agreement.

B. Duration: For the Term and any data retention required by law.

C. Nature and Purpose: Operation, maintenance, configuration, support, security monitoring, logging, analytics strictly for service operations, and delivery of Service features.

D. Categories of Data Subjects: Authorized users and personnel of Customer (employees, temporary workers, contractors) and, where applicable, authorized users of Customer's customers (for MSP scenarios).

E. Categories of Personal Data: Identification and contact data (name, business email/phone), account credentials and audit logs, technical identifiers (IP address, device/user IDs), and other data described in order forms. Special categories are not intended unless expressly agreed in writing.

F. Frequency of Transfer: Continuous as necessary for the Services.

G. Retention: As set out in Section 12 (RETURN AND DELETION) and the Agreement.

H. Data Location and Transfers: Customer Personal Data is stored and processed in the United States. Based on the configuration of the Services, Company does not intentionally transfer Customer Personal Data outside the United States.

Exhibit 2 — Technical and Organizational Measures (Annex II)

1. Information Security Program aligned to ISO/IEC 27001/27002.

2. Encryption of data in transit (TLS 1.2+) and at rest (AES-256 or equivalent); centralized key management with access separation.

3. Identity and Access Management: least-privilege, MFA, strong authentication, periodic access reviews, JIT elevation for admin tasks.

4. Network Security: segmentation, firewalls, IDS/IPS, secure baseline configurations, vulnerability scanning, patch management.

5. Application Security: SSDLC, code reviews, dependency scanning, secrets management, change management.

6. Monitoring & Logging: centralized logging, tamper-evident audit trails, anomaly detection, documented event escalation.

7. Business Continuity & Disaster Recovery: RPO/RTO targets, tested backups and recovery, redundancy for critical services.

8. Supplier Management: risk-based onboarding, security due diligence, contractual flow-down, continuous oversight.

9. Personnel Security & Training: background checks where lawful, privacy/security training, confidentiality obligations.

10. Penetration Testing: at least annually by independent testers; remediation tracking.

11. Data Minimization & Pseudonymization where feasible.

12. Secure Deletion: industry-standard data sanitization for media and logical deletion from backups within retention cycles.

Exhibit 3 — Authorized Sub-processors (Template)

Provider name; service description; location(s); data categories; transfer mechanism; security attestations (e.g., ISO 27001, SOC 2 Type II); DPA contact.

Schedule A — EU SCCs Incorporation (By Reference)

The Parties incorporate the EU 2021 SCCs (Module Two: Controller-to-Processor) by reference with the selections in Section 7.2 and the information in Exhibit 1 and Exhibit 2. The Parties will adopt any additional SCCs approved by the European Commission that address transfers to importers subject to the GDPR when instructed by Customer.

Schedule B — UK IDTA / UK Addendum Incorporation (By Reference)

For UK transfers, the UK IDTA or the UK Addendum to the EU SCCs is incorporated with Party details and annexes as set out in Exhibit 1 and Exhibit 2. The Parties shall complete any tables/appendices as reasonably required.

Schedule C — Swiss FADP Rider

The 2021 EU SCCs apply with the following Swiss-specific modifications: references to GDPR are read as FADP where applicable; the FDPIC is the competent authority; Swiss Data Subjects may enforce rights in Switzerland; where both GDPR and FADP apply, dual supervisory competence is recognized.

[END OF DOCUMENT]