DATA PROCESSING AGREEMENT

This Data Processing Agreement (the “DPA”) forms part of the applicable Master Services Agreement, Order, or Service Description (the “Principal Agreement”) between LMA Telecommunications, Inc. Dba Convergent Networks (the “Processor”), and Client (sometimes referred to as “you,” or “your,” or the “Controller”). This DPA is entered into and effective as of the last dated signature below.

The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect. In the event of a conflict between this DPA and the provisions of related agreements, including the Principal Agreement, the terms of this DPA shall prevail.

1. Definitions

In this DPA, the following terms shall have the meanings set out below:

1.1. “Anonymous Data” means information that relates to a group or category of consumers and/or individuals, from which: (i) the Controller cannot be identified as the source of the information; (ii) personally identifiable information allowing the identification of individuals is removed; and (iii) the information is not reasonably identifiable or linkable to any consumer, individual, household, or device.

1.2. “Applicable Laws” means data protection and privacy laws and regulations currently in effect and in force, solely to the extent applicable to Processor’s Processing of Personal Data on behalf of Controller and pursuant to the Principal Agreement in the jurisdictions where Processor’s Services are provided. Applicable Laws may include, where applicable, the GDPR and the CCPA.

1.3. “Personal Data” means any information that is reasonably associated or linked with an identified or identifiable person, and which is Processed by the Processor on behalf of the Controller pursuant to the Principal Agreement.

1.4. “CCPA” means the California Consumer Privacy Act of 2018.

1.5. "GDPR" means EU General Data Protection Regulation 2016/679 and 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 of 2018.

1.6. "Restricted Transfer" means the disclosure, grant of access, or other transfer of Personal Data to: (i) in the context of the European Economic Area ("EEA"), any country or territory outside the EEA that does not benefit from an adequacy decision from the European Commission (an "EEA Restricted Transfer"); and (ii) in the context of the United Kingdom ("UK"), any country or territory outside the UK that does not benefit from an adequacy decision from the UK government (a "UK Restricted Transfer").

1.7. "Services" means the services and other activities to be supplied to or carried out by or on behalf of Processor for Controller pursuant to the Principal Agreement.

1.8. "Standard Contractual Clauses" or "SCCs" means Commission Decision 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.

1.9. "Subprocessor" means any person (including any third party but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of Processor to Process Personal Data on behalf of any Controller in connection with the Principal Agreement.

1.10. "UK Addendum" means Version B1.0 of the International Data Transfer Addendum to the EU Commission's Standard Contractual Clauses, as issued by the UK's Information Commissioner's Office under S119A(1) Data Protection Act 2018 and in force 21 March 2022.

1.11. The terms "Data Protection Impact Assessments," "Data Subject," "Personal Data Breach," "Process," "Sell," "Share," and "Supervisory Authority" shall have the same meaning as in Applicable Laws.

2. Processing of Personal Data

2.1. Processor shall:

2.1.1. comply with all Applicable Laws in the Processing of Personal Data; and

2.1.2. not Process Personal Data other than on the Controller's documented lawful instructions unless Processing is required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform the Controller of that legal requirement before the relevant Processing of that Personal Data.

2.2. Controller shall:

2.2.1. instruct Processor (and authorizes Processor to instruct each Subprocessor) to:

2.2.1.1. Process Personal Data as described in Annex I; and

2.2.1.2. in particular, transfer Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Principal Agreement.

2.3. Controller represents and warrants that:

2.3.1. it has complied, and will continue to comply, with all Applicable Laws in respect of its Processing of Personal Data and any Processing instructions issued to Processor;

2.3.2. it is and will at all relevant times remain duly and effectively authorized to give the instructions set out in this section;

2.3.3. it has all necessary rights to provide the Personal Data to the Processor for the Processing to be performed in relation to the Services;

2.3.4. one or more lawful bases set forth in the Applicable Laws support the lawfulness of the Processing;

2.3.5. all necessary privacy notices are provided to Data Subjects;

2.3.6. any necessary Data Subject consents to the Processing are obtained and a record of such consents is maintained; and

2.3.7. should such a consent be revoked by a Data Subject, and no other lawful basis remains to keep the Data Subject's Personal Data, it will communicate the fact of such revocation to the Processor.

2.4. Controller will ensure that Processor's Processing of the Personal Data in accordance with Controller's instructions will not cause Processor to violate any Applicable Law, regulation, or rule.

2.5. Processor acknowledges that it is a Service Provider and that all Personal Data that it may receive from Controller, Controller's employees or consultants, or otherwise acquired by virtue of the performance of Services under the Principal Agreement shall be regarded by Processor as strictly confidential and held by Processor in confidence.

2.6. Processor shall not directly or indirectly Sell or Share any Personal Data; not retain, use, or disclose any Personal Data for any purpose other than for the purpose of performing Services for Controller or as otherwise permitted under Applicable Laws; and not retain, use, or disclose any Personal Data outside the scope of this DPA or the Principal Agreement.

2.7. Processor shall not combine Personal Data received from Controller with Personal Data from any other source, including Personal Data obtained from other persons or Personal Data obtained by Processor itself from its own interactions with the consumer with whom the Personal Data is associated, provided that Processor may combine Personal Data to perform any business purpose authorized by Applicable Laws.

2.8. Processor shall notify Controller without undue delay if it makes the determination that it can no longer meet any of its obligations under this DPA.

2.9. Processor may use Anonymous Data for its own purposes.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Processor, ensuring that all such individuals are subject to appropriate confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1. 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, Processor shall in relation to the Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk.

4.2. In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

4.3. The Parties acknowledge that security requirements are constantly changing and that effective security may require improvements of outdated security measures. Controller will bear the cost, if any, to implement material changes required by specific updated security requirements set forth in Applicable Laws or by regulatory authorities of competent jurisdiction.

4.4. Where an amendment to the Principal Agreement is necessary in order to execute a Controller instruction to the Processor to improve security measures as may be required by changes in Applicable Laws from time to time, the Parties shall negotiate an amendment to the Principal Agreement in good faith.

5. Restricted Transfers

5.1. Processor shall not transfer Personal Data, or permit any such transfers in/from a country which constitutes a Restricted Transfer unless it takes the appropriate guarantees to ensure such transfer is in accordance with Applicable Laws. Such appropriate guarantees may consist of: (i) participation in the Data Privacy Frameworks or other adequacy decision; (ii) applicable standard data protection clauses pursuant to Article 46.2 c) or d) of the GDPR; (iii) binding corporate rules pursuant to Article 46.2 b) of the GDPR; (iv) derogations for specific situations under Article 49 of the GDPR; or, (v) any other instrument recognized by the GDPR and approved by the European Commission or a Supervisory Authority.

5.2. To the extent there is no adequacy decision and an EEA Restricted Transfer relies on the Standard Contractual Clauses, the Parties hereby agree to and incorporate the Standard Contractual Clauses in full, as follows:

5.2.1. Module Two will apply;

5.2.2. in Clause 7, the optional docking clause will apply;

5.2.3. in Clause 9, option 2 (general written authorization) will apply, and the time period for prior notice of Subprocessor changes shall be 30 days;

5.2.4. in Clause 17, the Standard Contractual Clauses will be governed by Irish law;

5.2.5. in Clause 18(b), disputes shall be resolved before the courts of Ireland;

5.2.6. Annexes I, II, and III of the Standard Contractual Clauses shall be deemed completed with the information set out in Annexes I, II, and III to this Addendum.

5.3. If a transfer constitutes a UK Restricted Transfer, the Parties hereby agree to and incorporate the UK Addendum in full, as follows:

5.3.1. Table 1 (Parties) shall be deemed completed with the information set out in Annex I to this Addendum;

5.3.2. in Table 2 (Selected SCCs, Modules and Selected Clauses), the Addendum EU SCCs shall be the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of the UK Addendum:

5.3.2.1. Module Two will apply;

5.3.2.2. in Clause 7, the optional docking clause will apply; and,

5.3.2.3. in Clause 9, option 2 (general written authorization) will apply, and the time period for prior notice of Subprocessor changes shall be 30 days;

5.3.3. in Table 3 (Appendix Information), Annexes I, II, and III shall be deemed completed with the information set out in Annexes I, II, and III to this DPA; and,

5.3.4. in Table 4 (Ending this Addendum when the Approved Addendum Changes), both the Importer and Exporter may end the UK Addendum.

6. Subprocessing

6.1. Controller authorizes Processor to appoint (and permit each Subprocessor appointed in accordance with this section to appoint) Subprocessors in accordance with this section and any restrictions in the Agreement.

6.2. Processor may continue to use those Subprocessors already engaged by Processor as of the date of this Addendum, as set forth in Annex III. Processor may update the list of Subprocessors from time to time.

6.3. With respect to each Subprocessor, Processor shall ensure that the arrangement between Processor, on the one hand, and the Subprocessor, on the other hand, is governed by a written contract containing provisions that are substantially similar as the obligations set forth in this DPA, to the extent applicable to the nature of the service provided by such Subprocessor.

7. Data Subject Rights

7.1. Taking into account the nature of the Processing, Processor shall assist each Controller by implementing appropriate technical and organizational measures, insofar as this is feasible, for the fulfilment of the Controller’s obligations to respond to requests to exercise Data Subject rights under the Applicable Laws.

7.2. Processor shall:

7.2.1. notify Controller if Processor receives a request from a Data Subject under any Applicable Laws in respect of Personal Data; and

7.2.2. ensure that the Processor does not respond to that request except as required by Applicable Laws to which the Contracted Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Controller of that legal requirement before the Contracted Processor responds to the request.

7.3. Controller shall be responsible for responding to a request from a Data Subject as required under any Applicable Laws in respect of Personal Data.

8. Assistance to Controller

To the extent required under Applicable Laws, and taking into account the nature of Processing and the information available to the Processor, the Processor shall assist the Controller in required Data Protection Impact Assessments, and with prior consultations with Supervisory Authorities.

9. Personal Data Breach

In the event of a Personal Data Breach, Processor shall notify Controller without undue delay and provide a non-privileged, factual summary of the Personal Data Breach. Controller is solely responsible for complying with incident notification laws applicable to Controller and fulfilling third party notification obligations related to any Personal Data Breach (e.g., Article 33 and 34 of the GDPR).

10. Audits

10.1. To the extent audits are required by Applicable Laws or requested by a regulatory authority of competent jurisdiction, Controller shall provide Processor with 30 days’ written notice of the audit and shall identify the relevant requirement or request in its notice to Processor of the audit. The Parties shall negotiate in good faith the time, manner, and scope of such an audit and the audit shall be conducted at Controller’s sole expense, including without limitation the personnel costs of Processor for personnel involved in an audit of Controller. Processor may provide copies of its policies and procedures and written responses to Controller's questions for purposes of such an audit. Under no circumstances shall Controller have or require logical or administrative access to Processor's systems, access to the confidential information of Processor's other customers, or access to Processor's proprietary information. All information provided during such audits shall be treated as Processor’s confidential information, and Controller shall ensure that such protections satisfactory to Processor are in force prior to the initiation of any audit.

10.2. Processor need not give access to its premises or records for the purposes of such an audit:

10.2.1. to any individual unless he or she produces reasonable evidence of identity and authority;

10.2.2. outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the Controller undertaking an audit has given notice to Processor that this is the case before attendance outside those hours begins; or

10.2.3. for the purposes of more than one audit or inspection in any calendar year, except for any additional audits or inspections which the Controller is required or requested to carry out by Applicable Laws or a regulatory authority of competent jurisdiction, where the Controller has identified the relevant requirement or request in its notice to Processor of the audit or inspection.

11. Deletion or Return of Personal Data

11.1. Within 30 days of the termination date, Controller may by written notice request Processor either (a) return a complete copy of all Personal Data to Controller and/or (b) delete and procure the deletion of all other copies of Personal Data Processed by the Processor.

11.2. Processor may retain Personal Data to the extent required by Applicable Laws and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws.

12. Governing Law and Jurisdiction

12.1. The Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Principal Agreement; and,

12.2. This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

13. General

13.1. If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

13.2. The obligations placed upon either party under this DPA shall survive so long as Processor and/or its Subprocessors Processes Personal Data on behalf of Controller.

13.3. Processor may update this DPA from time to time to make changes as required by Applicable Laws and changes will be adopted upon notice to Controller.

IN WITNESS WHEREOF, the Parties have executed this DPA as of the last dated signature set forth below.

Convergent Networks	[CLIENT]
Name:	Name:
Title:	Title:
Date:	Date:
Signature:	Signature:

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name:	[CLIENT]
Address:	
Contact person’s name, position and contact details:	
Activities relevant to the data transferred under the Clauses:	As described in the Principal Agreement.
Signature and date:	
Role (controller/processor)	Controller

Data importer(s):

Name:	LMA Telecommunications, Inc. Dba Convergent Networks
Address:	12518 East Beverly Blvd Whittier, CA 90601
Contact person’s name, position and contact details:	
Activities relevant to the data transferred under the Clauses:	As described in the Principal Agreement.
Signature and date:	
Role (controller/processor)	Processor

B. DESCRIPTION OF THE TRANSFER

Categories of Data Subjects whose Personal Data is transferred

- End-Users of Controller
- Employees of Controller

- Contractors, Agents, or Representatives of Controller

Categories of Personal Data transferred

- Controller Customer
  - Name
  - Email
  - Phone number
- Controller Employee/ Contractor/ Agent/ Representative
  - Name
  - Email address and other business contact data
  - Name and location of employer
  - Unique User IDs

Special categories of Personal Data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

- Data will be transferred for the duration of the Principal Agreement.

Nature of the processing.

- Processor provides technology solutions to protect Controller's technology assets, data, and reputation.

Purpose(s) of the data transfer and further processing.

- The Personal Data transferred will be processed for the provision of the Services as specified in the Principal Agreement.

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period.

- The Personal Data transferred will be retained for as long as necessary for the provision of the Services as specified in the Principal Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13.

- Irish Data Protection Commission.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Compliance Program

Provider has developed written privacy and security policies and procedures to document its data protection practices.

Anti-Intrusion Security

Provider implements and monitors intrusion prevention and detection systems.

Access Controls and Identity Management

Provider implements measures to prevent unauthorized physical access such as locks/keys and electronic access through credential checking. Access to data is further designated based upon a need-to-know basis.

Encryption

Provider uses industry recognized standards to encrypt data at rest (AES 256) and in transit (TLS 1.2).

Incident Response Plan

Provider maintains a written incident response plan.

Contractual Obligations on Vendors and Contractors

Provider enters into agreements to protect the confidentiality and security of Client Personal Data.

Contractual Obligations on Employees

As a part of employment agreement/employee handbooks, Provider’s employees are obligated to protect the confidentiality and security of Client’s Personal Data.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Entity name	Country where processing is performed	Description of processing