DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is made as of the date of the Service Agreement between Customer and and CallTower, Inc. a Utah Corporation, with its principal offices located at 10701 River Front Parkway, 4th Floor, South Jordan, Utah 84095, United States and its affiliates, including Inoria, Inc. located at 1255 Phillips Square, Suite 307, Montreal, Quebec, Canada H3B3G1 and CallTower UK Ltd. located at 5th Floor, Halo, Counterslip, Bristol BS1 6AJ, United Kingdom ("Processor") (each a "Party", and together the "Parties").

RECITALS

WHEREAS, the Parties have entered into a Service Agreement ("Agreement");

WHEREAS, the Parties wish to incorporate this DPA into the Agreement;

WHEREAS, in the course of providing the Services to Customer pursuant to the Agreement, Processor may Process Personal Data on behalf of Customer;

WHEREAS, to ensure adequate safeguards with respect to the Processing of Personal Data provided by Customer to the Processor the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

NOW, THEREFORE, in consideration of the foregoing premises and of the mutual promises and covenants set forth below, Customer and Processor hereby agree as follows:

AGREEMENT

1. DEFINITIONS

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. The term "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Applicable Data Protection Laws**" means all applicable laws, regulations, regulatory guidance, or requirements in any jurisdiction relating to data protection, privacy, or confidentiality of Personal Data including but not limited to (a) the EU General Data Protection Regulation (EU) 2016/679 ("GDPR") together with any transposing, implementing or supplemental legislation, and (b) the California Consumer Privacy Act ("CCPA").

Authorized Affiliate" means any of Customer's Affiliates which (a) are subject to the data protection laws and regulations of the European Economic Area and/or its member states,

the United Kingdom, and Switzerland, (b) are subject to data protection laws and regulations outside of the European Economic Area and/or its Member States, Switzerland, and the United Kingdom (as applicable), and (c) permitted to use Processor for Processing pursuant to the Agreement;

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data. For the avoidance of doubt, the Party identified as Customer above is a Controller under this DPA.

"Data Breach" means a breach of security leading to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, access to, or other Processing of Personal Data transmitted, stored, or otherwise Processed.

"Data Protection Authority" means any representative or agent of a government entity or agency who has the authority to enforce Applicable Data Protection Laws.

"Data Subject" means a natural person to whom Personal Data relates.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable natural person or particular household. An identifiable natural 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.

"Process" shall mean any operation or set of operations which is performed upon Personal Data by the Parties or in connection with and for the purposes of the provision of the Services, whether or not accomplished by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; and as defined by Applicable Data Protection Laws.

"Processor" means the entity which Processes Personal Data on behalf of the Customer. For the avoidance of doubt, the Party identified as "Processor" above is a Processor for this DPA.

"Services" means Processing of Personal Data by the Processor in connection with and for the purposes of the provision of the services to be provided by the Processor pursuant to the Parties Agreement.

"Service Provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that process information on behalf of a Data Controller and to which the Data Controller discloses a Data Subject's Personal Data for a Business Purpose pursuant to a written contract, provided that the contract prohibits the Service Provider from retaining, using, or disclosing the Personal Data for any purpose other than for the specific purpose of performing the services specified in the contract, or as otherwise permitted by the CCPA, including retaining, using, or disclosing the Personal Data for a Commercial Purpose other than providing the services specified in the contract with the Data Controller. The terms "Business Purpose" and "Commercial Purpose" have the same meaning as those terms are used in the CCPA. For the avoidance of doubt, Processor is a Service Provider.

"Sub-processor" means any entity which Processes Personal Data on behalf of the Processor.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The party identified above as Customer is a Controller under this DPA. The party identified above as Processor is a Processor under this DPA. The subject matter, duration, purpose of the Processing, and the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1. The Parties agree that this DPA is incorporated into the Agreement.

2.2 Customer's Obligations. Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquires Personal Data and provides it to Processor.

2.3 Processor's Obligations. All Personal Data Processed by Processor pursuant to the Agreement is Confidential Information and Processor will Process Personal Data only in accordance with Customer's documented instructions set forth in Schedule 1 or as otherwise provided by Customer in writing. Processor will not sell the Personal Data Processed under this DPA and will not retain, use, or disclose Personal Data outside of the direct business relationship between Processor and Customer. Processor shall adhere to all Applicable Data Protection Laws with regard to Processing Personal Data. Where the Processor believes that compliance with any instructions by Customer would result in a violation of any Applicable Data Protection Law, the Processor shall notify Customer thereof in writing without delay. Processor shall make available to the Customer all information necessary to demonstrate Processor's compliance with its obligations under this DPA.

2.3.1. Assistance Requirements. Processor shall assist Customer with the following: compliance with Applicable Data Protection Laws when required by Applicable Data Protection Laws; suspected and relevant Data Breaches; notifications to, or inquiries from a Data Protection Authority; notifications to, and inquiries from, Data Subjects; and Customer's obligation to carry out data protection impact assessments and prior consultations with a Data Protection Authority.

3. NOTIFICATION OBLIGATIONS

3.1 Processor's Notification Obligations. Processor shall immediately notify Customer, in writing, of the following:

3.1.1 A Data Subject's request to exercise their privacy rights such as accessing, rectifying, erasing, transporting, objecting to, or restricting their Personal Data;

3.1.2 Any request or complaint received from Customer's customers or employees;

3.1.3 Any question, complaint, investigation, or other inquiry from a Data Protection Authority;

3.1.4 Any request for disclosure of Personal Data that is related in any way to Processor's Processing of Personal Data under this DPA;

3.1.5 A Data Breach pursuant to the notification obligations set forth in Section 7.1; and

3.1.6 Where the Personal Data becomes subject to search a seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being Processed.

Processor will assist Customer in fulfilling Customer's obligations to respond to requests relating to sections (3.1.1)-(3.1.6) above and will not respond to such requests without Customer's prior written consent unless Processor is required to respond by applicable law.

4. CONFIDENTIALITY

4.1 Confidential Information. All Information provided to Processor pursuant to the Agreement is Confidential Information.

4.2 Processor's Personnel. Processor shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. Processor shall ensure that such confidentiality obligations survive the termination of their respective employment relationship with such individuals.

4.3 Limitation of Access. Processor shall ensure that Processor's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that Processor and Processor's Affiliates may engage third-party Sub-processors in connection with the provision of the Services. Processor or Processor's Affiliate shall enter into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2 Notification of Changes to Sub-processors. Processor will inform Customer of any intended changes concerning the addition or replacement of Sub-processors and give Customer an opportunity to object to such changes. Processor will notify Customer of any intended changes concerning the addition or replacement of Sub-processors in writing at least 30 days prior to its use of the Sub-processor.

5.3 Objection Right for New Sub-processors. Customer may object to Processor's use of a new Sub-processor by notifying Processor promptly in writing within fifteen (15) business days after receipt of Processor's notice. In the event Customer objects to a new Sub-processor, Processor will use reasonable efforts to make available to Customer a change in the Services to avoid Processing of Personal Data by the objected-to new Sub- processor. If Processor is unable to make available such change, Customer may terminate the applicable Agreement with respect to those Services which cannot be provided by Processor without the use of the objected-to new Sub-processor.

5.4 Liability for Acts of Sub-Processors. Processor shall be liable for the acts and omissions of its Sub-processors to the same extent Processor would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

6. SECURITY

6.1 Protection of Personal Data. Processor shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data.

6.2 Audit Rights. Customer, or Customer's designee, has the right to audit and inspect—at Customer's expense—Processor's premises, policies, procedures, and computerized systems to make sure Processor complies with the requirements in this DPA. Customer, or Customer's designee, will provide at least 72 hours notification before conducting an audit unless such audit is required due to a Data Breach involving Processor. Audits by Customer or Customer's designee will not violate Processor's confidentiality obligations with Processor's other clients.

7. DATA BREACHES

7.1 Data Breach Notification. Processor shall notify Customer in writing without undue delay after becoming aware of a suspected Data Breach. In no event shall such notification be made more than 24 hours after Processor's discovery of the Data Breach.

7.2 Data Breach Management. Processor shall make reasonable efforts to identify the cause of such Data Breach and take those steps as Processor deems necessary and reasonable to remediate the cause of such a Data Breach to the extent the remediation is within Processors reasonable control.

8. TERMINATION

8.1 Termination. This DPA shall terminate automatically upon the later of (a) the termination or expiry of the Agreement or (b) Processor's deletion or return of Personal Data. Customer shall further be entitled to terminate this DPA for cause if the Processor is, in the sole opinion of Customer, in a material or persistent breach of this DPA which, in the case of a breach capable of remedy, shall not have been remedied within ten (10) days from the date of receipt by the Processor of a notice from Customer identifying the breach and requesting its remedy.

8.2 Return or Deletion of Data. Upon termination of this DPA, Processor will delete or return all existing copies of Personal Data unless applicable law requires continued retention of the Personal Data. Upon the request of Customer, the Processor shall confirm compliance with such obligations in writing and delete all existing copies. In instances where applicable law requires the Processor to retain Personal Data, Processor will protect the confidentiality, integrity, and accessibility of the Personal Data; will not actively Process the Personal Data; and will continue to comply with the terms of this DPA.

9. MECHANISMS FOR INTERNATIONAL TRANSFERS

9.1 Transfers Outside of the EU. During the provision of Services under the DPA, it may be necessary for Customer to transfer Personal Data from the European Union, the European Economic Area and/or their member states, the United Kingdom, or Switzerland to Processor in a country that does not have an adequacy decision from the European Commission or is not located in the European Economic Area. In case of such a transfer, the Standard Contractual Clauses apply as follows:

9.1.1. In relation to Personal Data that is subject to the GDPR (i) Processor will be deemed the "data importer" and Customer is the "data exporter"; (ii) the Module Two terms shall apply where Customer is a Data Customer and where Processor is a Data Processor; (iii) in Clause 7, the optional docking clause shall be deleted; (iv) in Clause 9 of Module Two, Option 2 shall apply and the list of Subprocessors and time period for notice of changes shall be as agreed under Section 5 of this DPA; (v) in Clause 11, the optional language shall be deleted; (vi) in Clause 17, Option 1 shall apply and the Standard Contractual Clauses shall be governed by the member state where Customer is domiciled; (vii) in Clause 18(b), disputes shall be resolved before the courts of the member state where Customer is domiciled; (viii) Annex I and Annex II shall be deemed completed with the information set out in Schedule 1 of this DPA respectively; and (ix) if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict. For this section, the Standard Contractual Clauses from the Commission Implementing Decision (EU) 2021/914 are incorporated by reference and available here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

9.1.2. In relation to Personal Data that is subject to UK Data Protection Laws, the International Data Transfer Agreement ("IDTA") shall apply with the following modifications: (i) the contact information about the parties to the Agreement is the contact information for the IDTA; (ii) Customer is the data exporter and

Processor is the data importer; (iii) the laws that govern the IDTA and the location where legal claims can be made is England and Wales; (iv) the UK GDPR does not apply to the data importer's processing of transferred data; (v) the Parties do not use the additional security or commercial clauses from the IDTA; and (vi) the information in this DPA and Schedule 1 can be used for Tables 1-4. For this section, the Standard Contractual Clauses from the Information Commissioner's Office are incorporated by reference and available here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

9.1.3. In relation to Personal Data that is subject to the Swiss DPA, the Standard Contractual Clauses referenced in Section 9.1.1 shall apply with the following modifications (i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA; (ii) references to "EU", "Union" and "Member State law" shall be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" shall be replaced with the "the Swiss Federal Data Protection and Information Commissioner " and the "relevant courts in Switzerland".

9.2. Alternative Data Transfer Mechanisms. The Parties acknowledge that the laws, rules and regulations relating to international data transfers are rapidly evolving. If Customer adopts another mechanism authorized by applicable laws, rules or regulations to transfer Personal Data (each an "Alternative Data Transfer Mechanism"), the Parties agree to work together in good faith to implement any amendments to this Agreement necessary to implement the Alternative Data Transfer Mechanism.

If a law or regulation replaces or supersedes any of the standard contractual clauses referenced in this Section, the Parties may adopt the text of the new standard contractual clauses without having to amend this DPA.

10. MISCELLANEOUS PROVISIONS

10.1. Amendments. This DPA may not be amended or supplemented, nor shall any of its provisions be deemed to be waived or otherwise modified, except through a writing duly executed by authorized representatives of both Parties.

10.2 Governing Law. This DPA shall be governed by the governing law set forth in the Agreement.

List of Schedules:

Schedule 1: Description of the Processing

SCHEDULE 1

Description of the Processing

Contact Information
Customer's information and details are listed in the Agreement

CallTower, Inc.
Address: 10701 River Front Parkway, 4th Floor, South Jordan, UT 84095
Representative/DPO/Privacy Office Email: privacy@calltower.com

Subject-Matter
The subject-matter of the Processing:
As set forth in the Agreement between the Parties.

Duration
Duration of the Processing:
As set forth in the Agreement between the Parties.

Extent, Type and Purpose of the Processing
The extent, type and purpose of the Processing is as follows:
As set forth in the Agreement between the Parties.

Frequency of Transfer
☒Continuous
☐One-off

Data Subjects
Personal Data Processing may relate to the following categories of Data Subjects:
Personal Data Processing will pertain to customers' employees. Limited public personal information from people who call our customers' business communications systems.

Subprocessor Transfers
Fill out the chart below for each Subprocessor engaged by Processor. Controller approves the use of each Subprocessor listed.

Subprocessor Name	Subprocessor's Location	General description of what will be processed and how
Bandwidth/Voxbone	Various – Headquartered in USA	PSTN operator to connect calls to / from customer telephone numbers
DIDWW	Various – Headquartered in Ireland	PSTN operator to connect calls to / from customer telephone numbers
NTT Global	Various – Headquartered in USA	PSTN operator to connect calls to / from customer telephone numbers

Colt	Various – Headquartered in UK	PSTN operator to connect calls to / from customer telephone numbers
Fibernetics	Various – Headquartered in Canada	PSTN operator to connect calls to / from customer telephone numbers
X3i Solutions	Various –Headquartered in USA	PSTN operations support including number porting
382Com	Various – Headquartered in USA	PSTN operator to connect calls to / from customer telephone numbers
Telestra	Various – Headquartered in USA	PSTN operator to connect calls to / from customer telephone numbers
Virtual-Call	Various – Headquartered in Switzerland	PSTN operator to connect calls to / from customer telephone numbers
Verizon	Various – Headquartered in USA	PSTN operator to connect calls to / from customer telephone numbers
Lumen	Various – Headquartered in USA	PSTN operator to connect calls to / from customer telephone numbers
Telefonica	Various – Headquartered in USA/Spain	PSTN operator to connect calls to / from customer telephone numbers
Sinch	Various – Headquartered in USA	PSTN operator to connect calls to / from customer telephone numbers
CommsGroup	Various – Headquartered in Australia	PSTN operator to connect calls to / from customer telephone numbers
Peerless Networks	Various – Headquartered in USA	PSTN operator to connect calls to / from customer telephone numbers
Tata	Various – Headquartered in USA	PSTN operator to connect calls to / from customer telephone numbers
Microsoft	Various – Headquartered in USA	File storage, email, and communication applications
Rev.IO	United States	US-based billing management and invoice distribution
Salesforce	United States	CRM, Project, and trouble ticket management for CallTower employees
GuideCX	United States	Project management application for CallTower employees

ClientSuccess	United States	CRM integration for Salesforce
HubSpot	United States	Opt-in marketing content distribution
Atlassian	Australia	Opt-in email notification system and project time tracking system
Linksquares	United States	Contract management
Pandadoc	United States	Contract presentation and e-signature
Hubspot	United States	Opt-in marketing content distribution
BlueOps	United States	Data Analytics
Intralinks	United States	Data Storage and Analytics

Categories of Data

The Personal Data Processed may concern the following categories of data:

☒Identifying Information
☒Social and Contact Information
☐Financial Data
☐Tracking Data
☐Personal History
☐Opinions, Beliefs, and Personal Preferences
☐Sensitive Data

Technical Measures to Secure Data

Security Awareness Training

Processor has security awareness training which includes mandatory security training about the handling and securing of confidential information and sensitive information such as personally identifiable information, financial account information, and health information consistent with applicable law, and periodic security awareness communications and security courses that focus on end-user awareness.

Security Policies and Procedures

Processor has information security, use and management policies which dictate the actions of employees and contractors regarding appropriate use, access to and storage of confidential and sensitive information; restrict access to confidential and sensitive information to members of Processor's workforce who have a "need to know" such information; prevent terminated employees from accessing Processor's information post-termination; and impose disciplinary measures for failure to abide by such policies. System access to Processor resources denied unless specifically assessed and access granted. Processor performs background checks of its employees at time of hire, as permitted by law.

Physical and Environmental Access Controls

Processor limits physical access to its information systems and facilities using physical controls (e.g., coded pass access) that provide reasonable assurance that access to its data centers is limited to authorized individuals and employs camera or video surveillance systems at critical internal and external entry points. Processor applies air temperature and humidity controls for its data centers and protects against loss due to power failure.

Logical Access Controls

Processor employs logging and monitoring technology to help detect and prevent unauthorized access attempts to its networks and production systems. Processor's monitoring includes a review of changes affecting systems' handling authentication, authorization, and auditing; privileged access to Processor's production systems.

Encryption Controls

Processor applies business-appropriate encryption controls across our products. Processor evaluates and applies in-transit and at-rest encryption utilizing industry best practices for ciphers. Best practices are utilized for the lifecycle management of encryption keys, including generation, storage, access control, and rotation.

Vulnerability Management

Processor regularly performs vulnerability scans and addresses detected vulnerabilities in accordance with their risk. Processor products are also subject to periodic vulnerability assessment and penetration testing.

Disaster Recovery and Back-up Controls

Processor performs periodic backups of production file systems and databases according to a defined schedule and maintains a formal disaster recovery plan for the production cloud data center, including regular testing.

Cyber Incident Response Plan

Processor employs an incident response plan to manage and minimize the effects of unplanned cyber events that includes procedures to be followed in the event of an actual or potential security breach, including: an internal incident response team with a response leader; an investigation team performing a root causes analysis and identifying affected parties; internal reporting and notification processes; documenting responsive actions and remediation plans; and a post-incident review of events.

Storage and Transmission Security

Processor employs technical security measures to guard against unauthorized access to Processor data that is being transmitted over a public electronic communications network or stored electronically.

Secure Disposal

Processor employs policies and procedures regarding the disposal of tangible and intangible property containing Processor data so that Processor data cannot be practicably read or reconstructed.

Risk Identification & Assessment

Processor employs a risk assessment program to help reasonably identify foreseeable internal and external risks to Processor's information resources and determine if existing controls, policies, and procedures are adequate to address the identified risks.