DATA PRIVACY ADDENDUM FOR SERVICE PROVIDERS

This Consolidated Data Privacy Addendum for Vendors and Third-Party Representatives ("**DPA**") is incorporated by refence into and forms part of the Master Purchase Agreement ("MPA"), Master Services Agreement ("MSA"), Master Representative Agreement ("MRA"), Statement of Work ("SOW"), or Service, Product, or Purchase Order ("Order") (together with any appendices, exhibits, annexes, or amendments thereto, the "**Agreement**") executed between Consolidated Communications ("**Consolidated**") and the vendor, service provider, contractor, third-party representative, or Representative ("**Service Provider**") indicated in the applicable Agreement. Consolidated enters into this DPA on its own behalf and on behalf of its Affiliates.

1. Definitions. Capitalized terms used in this DPA shall have the meanings set forth in this DPA. Defined terms used in but not defined in this DPA shall have the meaning ascribed to them in the Agreement.

1.1. "**Access**" means: (a) to enter a location; or (b) to obtain, read, copy, edit, divert, release, affect, alter the state of, or otherwise view data or systems in any form, including through information technology (IT) systems, cloud computing platforms, networks, security systems, and equipment (software and hardware).

1.2. "**Affiliate**" means all entities that Control, are Controlled by, or are under common Control with a Party, where "**Control**" means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of an entity, whether through the ownership of at least fifty percent (50%) of its voting securities, by contract, or otherwise. Consolidated "Affiliates" are limited to subsidiaries under the direct and indirect Control of Consolidated.

1.3. "**Customer Proprietary Network Information**" or "**CPNI**" means (a) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of Consolidated; and information contained in the bills pertaining to their voice services or (b) as otherwise defined by 47 U.S.C. §222(h)(1).

1.4. "**Controller**" means the entity that determines the purposes of the Processing of Personal Data.

1.5. "**Data Privacy Laws**" means all United States federal, state, or local laws and regulations relating to Personal Data, as they may be amended or replaced. Data Privacy Laws includes laws and regulations that are enacted or become effective after the Effective Date.

1.6. "**Data Subject**" means the identified or identifiable natural person to whom the Personal Data relates and includes any similarly defined term under Data Privacy Laws.

1.7. "**Foreign Person**" or "**Foreign Personnel**" means Personnel or Service Provider Personnel who are not United States citizens.

1.8. "**Personal Data**" means information (regardless of form) that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, and as may be further defined under Data Privacy Laws, and includes CPNI and information that constitutes "personal information," "personal data," "personally identifiable information," or any similarly defined term under Data Privacy Laws.

1.9. "**Personnel**" or "**Service Provider Personnel**" means (a) all employees, agents, contractors and/or subcontractors of Service Provider, and (b) all subcontractors' respective employees, agents and contractors who provide any portion of the Provided Services in connection with the Agreement, and (c) all Service Provider's Subprocessors.

1.10. "**Provided Services**" means any and all products or services provided by Service Provider to Consolidated pursuant to the Agreement.

1.11. "**Processing**" means any operation or set of operations performed on Personal Data, whether or not by automatic means. Processing includes, but is not limited to, access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making Personal Data available. The terms "Process," "Processes," and "Processed" have the same meaning as Processing under this DPA.

1.12. "**Processor**" means an entity that Processes Personal Data on behalf of a Controller and includes any similarly defined term under Data Privacy Laws.

1.13. "**Sale**" or "**Sell**" means the transfer, disclosure, dissemination, or other exchange of Personal Data for monetary or other valuable consideration.

1.14. "**Security Incident**" means any actual or reasonably suspected (a) accidental or unauthorized access, acquisition, alteration, destruction, disclosure, loss, modification, processing, or storage of Personal Data; (b) activity that results in an unauthorized disruption or denial of Consolidated's services; or (c) unauthorized access or modification to Consolidated's systems or systems used to access, process, or store Consolidated Data or Consolidated's systems or networks.

1.15. "**Subprocessor**" means any entity engaged by Service Provider to Process Personal Data.

1.16. "**U.S. Records**" means Consolidated's customer billing records, customer/subscriber information, personally identifiable information, sensitive Personal Data (as defined by Data Privacy Laws or 31 C.F.R. § 800.241), call detail records, internet protocol data records, CPNI, geolocation data, and any other information used, processed, or maintained in the ordinary course of business related to the services offered by Consolidated within the United States, including information subject to disclosure to a U.S. federal or state governmental entity under the procedures set forth in 18 U.S.C. § 2703(c), (d) and 18 U.S.C. § 2709.

2. **Roles of the Parties.** The parties agree that with respect to Service Provider's Processing of Personal Data, Consolidated is the "Controller", and Service Provider is the "Processor.".

3. **Scope of Processing.** The nature and purpose of the Processing are established in the Agreement. The duration of Processing is for the duration of the Agreement (or as otherwise defined in the Agreement). The types of Personal Data subject to Processing under this DPA are described in Annex A.

4. **Data Privacy Laws.** Service Provider will comply with Data Privacy Laws and protect Personal Data as required by Data Privacy Laws and this DPA. Consolidated has the right to take reasonable and appropriate steps to help ensure that Service Provider uses Personal Data in a manner consistent with Consolidated's obligations under Data Privacy Laws. If Service Provider reasonably determines that it is unable to meet its obligations under Data Privacy Laws and this DPA, Service Provider will notify Consolidated without undue delay. Consolidated has the right, upon becoming aware, including via notice pursuant to the preceding sentence, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data, including, without limitation, by directing Service Provider to suspend its Processing of Personal Data. Any such suspension will continue until Service Provider can meet its obligations under Data Privacy Laws and this DPA. However, if, in Consolidated's sole determination, Service Provider cannot meet its obligations under Data Privacy Laws and this DPA within a reasonable amount of time, Consolidated may terminate the Agreement for Service Provider's breach of this DPA. This breach and termination of the Agreement will be without penalty, additional cost, and liability to Consolidated, and without limiting Consolidated's remedies at equity and law, Service Provider shall promptly refund any unused, prepaid fees.

5. **Confidentiality.** Personal Data shall be considered Consolidated's Confidential Information. Service Provider shall hold Personal Data in strict confidence. Service Provider will not disclose Personal Data to any third party, including Service Provider's Affiliates, unless such disclosure is expressly permitted under the Agreement. Service Provider will not use Personal Data for its own purposes nor permit its use for any purposes of any third party. When disclosure of Personal Data is permitted, Service Provider shall: (a) limit access to Personal Data only to those entities and individuals, including Service Provider's Personnel, who need access to the relevant Personal Data, as strictly necessary for the purposes of performing the Agreement and to comply with Data Privacy Laws in the context of that entity's or individual's duties to Consolidated; (b) ensure that Service Provider Personnel who and third parties that Process Personal Data are subject to written obligations of confidentiality or are under an appropriate statutory obligation of confidentiality with respect to such Personal Data; and (c) ensure the reliability for maintaining confidentiality of any entity or individual engaged or employed in the Processing of Personal Data on behalf of Service Provider.

6. **Data Transfer.** Service Provider will not transfer Personal Data to or allow access to Personal Data by its Personnel or any third party in or from any location outside the United States without Consolidated's prior written approval.

7. **Security Measures.** Without limiting any data security provisions in the Agreement, Service Provider will implement and maintain industry best practices physical, administrative, and technical safeguards that protect the confidentiality, integrity, availability, and security of Consolidated Data, Consolidated's systems and, networks, and of Service Provider's systems and networks with access to Consolidated Data and are designed to prevent Security Incidents (the "**Security Measures**"). Such Security Measures shall: (a) be at least as protective as the measures Service Provider applies to its own similar information; (b) comply with Data Privacy Laws; and (c) without limiting the generality of the foregoing, include the security controls set forth in the Consolidated Security Addendum.

8. **Security Incident and Response.**
   8.1. Security Incident Response Plan. Service Provider shall implement and maintain an Incident Response Plan that enables Service Provider to (a) take actions to address any known or suspected Security Incident including ransomware, business email compromise, insider threat and data breach; (b) take appropriate remedial action; and (c) protect the confidentiality, integrity, and availability of Consolidated Data.
   8.2. Notification of Security Incident. In the event of a Security Incident, Service Provider shall notify Consolidated without undue delay, and in no event later than forty-eight (48) hours after the initial detection of a Security Incident by contacting Consolidated's Cyber Incident Response Team at network-security@consolidated.com. Such notification shall include all information necessary for Consolidated to expeditiously respond to the incident and comply with applicable Law, including, to the extent possible, (a) a description of the Security Incident, including the suspected cause, the nature of the information affected, the categories and approximate number of Data Subjects affected, the categories and approximate number of records involved, and a description of the current and any anticipated impact, and the likely consequences thereof; (b) the expected resolution time (if it has not already been resolved); (c) attack vector, if known; (d) whether a forensics company was engaged (e) corrective measures to be taken, evaluation of alternatives, and next steps; and (f) the name and phone number of the Service Provider that Consolidated may contact to obtain further information and updates.
   8.3. Response to Security Incident. At Service Provider's sole expense, Service Provider will (a) implement its Incident Response Plan; (b) promptly investigate and determine the exposures that led to the Security Incident; (c) take all necessary steps to eliminate or contain the exposure and prevent further incidents; (d) collect, preserve, and document evidence regarding the Security Incident, in each case in sufficient detail to meet reasonable expectations of forensic admissibility; and (e) provide Consolidated with all information, logs, or images reasonably requested by Consolidated in connection with the Security Incident, including, but not limited to, all information to allow Consolidated and each Consolidated Affiliate to meet any obligations to report or inform of the Security Incident under Data Privacy Laws and assess the risk to Consolidated, or Consolidated Data, including Personal Data. Service Provider will promptly provide Consolidated with updated notifications as it becomes aware of additional material information and regularly keep Consolidated apprised of the status of the Security Incident and all matters related to it.
   8.4. Cooperation. Service Provider shall cooperate with Consolidated's own response to and investigation of a Security Incident, and with any investigation relating to the Security Incident that is carried out by or at the direction of any government authority.
   8.5. Security Incident Notification Decision. Service Provider acknowledges and agrees that it is Consolidated's decision whether and when to disclose a Security Incident to affected individuals or regulators in the absence of any laws or regulations requiring Service Provider to report or notify.
   8.6. Public Statements. Service Provider shall not make any public statement about any Security Incident or Consolidated security vulnerability nor notify affected individuals of any Security Incident without Consolidated's prior written approval, unless Service Provider is required to do so pursuant to applicable Laws, in which case it shall provide Consolidated prior written notice of its intention to make such public statement or notify affected individuals.
   8.7. Costs of Remediation of Security Incidents. In the event of any Information Security Incident arising out of or relating to any (a) breach or alleged breach by Service Provider or by any Service Provider Personnel of the representations, warranties or covenants contained in this Security Addendum; (b) any Information

Security Incident; or (c) breach or alleged breach of Service Provider's obligations under this Security Addendum relating to privacy or security or caused by Service Provider's negligence or willful misconduct, Service Provider shall pay for or reimburse Consolidated for (i) expenses incurred to provide warning or notice to Consolidated's former and current employees, vendors, customers, and other persons and entities whose Personal Data or Confidential Information may have been disclosed or compromised as a result of the Security Incident (the "**Affected Persons**") and to law-enforcement agencies, regulatory bodies or other third parties as required to comply with law, or as otherwise directed by Consolidated; (ii) expenses incurred either directly by Consolidated or through Consolidated's retention of an independent third party forensic investigator, legal counsel, or any other third party, to investigate assess or remediate the Security Incident and to comply with applicable law and/or relevant industry standards; (iii) expenses related to the reasonably anticipated and commercially recognized consumer data breach mitigation efforts, including, but not limited to costs associated with the offering of credit monitoring for a period of at least twelve (12) months or such longer time as is required by law or recommended by one or more of Consolidated's regulators or any other similar protective measures designed to mitigate any damages to the Affected Persons; (iv) fines, penalties, or interest that Consolidated pays to any governmental or regulatory authority; (v) legal expenses incurred in connection with a Security Incident or to address any claims by third parties as a result of the Security Incident or investigation by law-enforcement agencies or regulatory bodies; and (vi) expenses incurred for the retention of a public relations or crisis management firm in order to manage communications on behalf of Consolidated related to any Security Incident.

9. **Service Provider's Assistance with Consolidated's Compliance.** Service Provider shall implement appropriate technical and organisational measures and other assistance reasonably necessary for Consolidated to comply with Data Privacy Laws, including, without limitation, as it relates to (a) conducting any data protection impact assessments, transfer impact assessments, or other assessments and (b) the security of Personal Data. Consolidated may take appropriate steps to ensure that Service Provider Processes Personal Data in a way that is consistent with Consolidated's obligations under Data Privacy Laws and Service Provider shall cooperate and assist Consolidated with such efforts. In the event of an investigation related to Service Provider's Processing of Personal Data, Service Provider will provide all assistance and support related to said investigation.

10. **Data Processing.** Service Provider will Process Personal Data solely for the provision of the Provided Services described in the Agreement and in accordance with lawful, documented instructions provided by Consolidated, except where otherwise required by law. Service Provider will provide prompt notice to Consolidated in the event Service Provider believes Consolidated's instructions violate Data Privacy Laws. The parties further acknowledge and agree that: (a) Consolidated's disclosure of Personal Data to Service Provider hereunder does not constitute a Sale and (b) Personal Data disclosed by Consolidated to Service Provider is provided to Service Provider only for the limited and specified purposes set forth in the Agreement and this DPA.

11. **Processing Restrictions.** Service Provider will not access, collect, retain, use, disclose, or otherwise Process Personal Data (a) outside the direct business relationship with Consolidated; or (b) for any purpose other than performing the Processing in accordance with this DPA and the Agreement. Service Provider will not rent, lease, or Sell Personal Data, or share it for targeted online advertising. Service Provider will not combine Personal Data with data received from or on behalf of any third party or collected by or on behalf of Service Provider, except as necessary for the Provision of the Provided Services.

12. **Personnel.**

    12.1. **Foreign Persons.** Prior to allowing a Foreign Person to engage in Processing any Personal Data, Service Provider will obtain Consolidated's approval as follows: (i) notify Consolidated at least forty-five calendar days in advance of such engagement and provide the Foreign Person's name, contact information, and nationality; (ii) complete the process for seeking approval of a Foreign Person's Access outlined in the

FCC Addendum; and (iii) should the Foreign Person not be approved to receive Access, work in good faith with Consolidated to find a replacement.

12.2. **Subprocessors.** Service Provider shall not disclose any Personal Data to any Subprocessor unless authorized by Consolidated. Authorized Subprocessors may be attached hereto as Annex B. Service Provider shall notify Consolidated in writing of the addition or replacement of any Subprocessor not set forth in Annex B or otherwise authorized at least forty-five (45) days prior to the proposed engagement. Consolidated may object to the proposed Subprocessor by providing Service Provider written notice of such objection. Upon receiving such an objection, Service Provider shall: (a) work with Consolidated in good faith to make available a commercially reasonable change in the provision of the Provided Services which avoids the use of that proposed Subprocessor or (b) take corrective steps requested by Consolidated in its objection. If Service Provider informs Consolidated that such change or corrective steps cannot be made, Consolidated may immediately terminate all or a portion of the Agreement for convenience and receive a refund of any prepaid fees. Service Provider shall engage a Subprocessor only pursuant to a written contract that (i) contains restrictions on Processing that are consistent with the terms of this DPA and compliant with Data Privacy Laws; and (ii) requires the Subprocessor to meet the obligations of Service Provider with respect to Personal Data. Service Provider shall be liable for all acts and omissions of the Subprocessor as if they were Service Provider's acts and omissions.

13. Individual Rights Requests.

13.1. **Requests from Individuals.** If Service Provider receives a request, inquiry, or complaint from or on behalf of an individual about Personal Data, Service Provider will promptly notify Consolidated of the request (but in any event no later than five (5) days after Service Provider receives such request), providing full details and circumstances of the request, inquiry, or complaint. Service Provider will not substantively respond to the request unless and as directed by Consolidated, unless otherwise required by law.

13.2. **Requests from Consolidated.** Service Provider will comply with Consolidated's reasonable requests for assistance in responding to Data Subject requests about Personal Data. Service Provider will comply with such requests without undue delay, and in any event within ten (10) calendar days of receipt of a written request from Consolidated.

14. Records and Audits. Service Provider shall establish and maintain complete and accurate records necessary to document compliance with this DPA and Data Privacy Laws, including, without limitation, accounts of all transactions involving Personal Data. Upon at least five (5) days' prior notice to Service Provider, Service Provider shall permit Consolidated, its auditors, designated Service Provider and regulators, to audit and inspect, at Consolidated's expense, and no more often than once per year (unless otherwise required by government regulators or applicable Laws, or unless a previous inspection revealed any deficiency): (a) the Service Provider's facilities where Personal Data is stored or maintained by or on behalf of Service Provider; (b) any computerized or paper systems used to share, disseminate, or otherwise Process Personal Data; (c) Service Provider's security practices and procedures related to Processing Personal Data; and (d) records required to be retained by Service Provider under this DPA, the Agreement, or applicable Laws.

15. Security Assessments. Consolidated may perform periodic security assessments, which may include assessment of certain portions of the systems involved in Processing Personal Data. Service Provider agrees to cooperate with, contribute to, and provide Consolidated with all information necessary to demonstrate the Service Provider's compliance with this DPA and Data Privacy Laws, at Service Provider's expense. Service Provider and Consolidated will mutually agree in advance on the scope, timing, and duration of any such assessments, including conditions of confidentiality.

16. Return or Deletion. Upon termination or expiration of the Agreement, Service Provider will securely return or delete all Personal Data, as Consolidated chooses, except to the extent Service Provider is expressly required by law to retain such Personal Data. Service Provider will notify Consolidated in writing when the data has been

deleted, if Consolidated chooses deletion. If Service Provider is legally required to retain Personal Data, Service Provider will provide Consolidated with a written notice that describes (a) the Personal Data that will be retained; (b) the legal justification for retaining the Personal Data; and (c) the security measures and the information retention period that Service Provider will apply to the Personal Data. Service Provider will securely return or delete the Personal Data, at Consolidated's option, when the legal justification for retaining the Personal Data no longer applies. Service Provider shall continue to protect all retained Personal Data consistent with the protections of this DPA and ensure that such Personal Data is only Processed as necessary for the purpose specified by such legal requirement and for no other purpose.

17. **Limitation of Liability.** Any limitations of liability in the Agreement do not apply to the Service Provider's obligations under this DPA.

18. **Indemnification.** Notwithstanding anything to the contrary in the Agreement and without regard to any limitations of liability contained in the Agreement, Service Provider shall indemnify and hold harmless Consolidated and Consolidated's Affiliates, employees, and agents from and against any and all liabilities, losses, damages, costs, and other expenses (including attorneys' and expert witnesses' costs and other legal fees) arising from or relating to Service Provider's breach of this DPA or violation of Data Privacy Laws. In the event of any third-party claim, demand, suit, or action (a "**Claim**") for which Consolidated (or any of Consolidated's Affiliates, employees, or agents) is or may be entitled to indemnification under this DPA, Consolidated may, at Consolidated's option, require Service Provider to defend such Claim at Service Provider's sole expense. Service Provider shall not settle any such Claim without Consolidated's express prior written consent.

19. **Breach.** A breach of this DPA is a material breach of the Agreement.

20. **Notifications.**

    20.1. Notifications of a Security Incident should be sent to network-security@consolidated.com using the subject line: Security Breach.
    20.2. Other notifications related to this DPA should be sent to network-security@consolidated.com using the subject line: Consolidated DPA Notice.

21. **Relationship to the Agreement**.

    21.1. The parties agree that this DPA replaces and supersedes any existing or prior DPA the parties may have previously entered into.
    21.2. Except as expressly modified herein, the terms of the Agreement shall remain in full force and effect.
    21.3. To the extent of any conflict or inconsistency between this DPA and any other document comprised within the Agreement, the order of precedence shall be, each when applicable, in descending order: 1) the Security Addendum, 2) this Data Privacy Addendum, 3) the FCC Addendum, 4) the amended master agreement, and 5) any Order or SOW.
    21.4. Under no circumstances shall an Order or SOW modify this DPA, unless such modification specifically references the term it is overriding and the document containing such modification is signed by both parties.
    21.5. This DPA will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Privacy Laws.

22. **Term.** The term of this DPA shall begin on the date last executed below and will end upon the later of (a) termination of the Agreement; or (b) Service Provider's destruction or return of all Personal Data Processed by Service Provider under the Agreement.

23. **General Provisions.** Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (a) amended as

necessary to ensure its validity and enforceability, while preserving the intent of the provision as closely as possible; or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein. Unless otherwise expressly stated herein, the parties will provide notices under this DPA in accordance with the Agreement.

Signed: Consolidated Communications	**Service Provider: _____**
By: _____	By: _____
Print Name: _____	Print Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Data Privacy Addendum Annex A: Details of Processing of Personal Data

Service Provider

Processor Details

Please provide contact details for processor.

Name	Service Provider, as defined in the DPA
Title / Role	As indicated for the Service Provider in the Agreement
Email	As indicated for the Service Provider in the Agreement
Phone Number	As indicated for the Service Provider in the Agreement

Complete the table below by checking off the applicable Data Subject or data element category.

	Customers	**Employees**	**Potential Customers and Others**
Personal Identifiers			
Name			
Email			
Street Address			
Existing Phone Number			
Account #			
Account Log in info (username, password)			
Online Identifiers			
Sensitive Personal Data			
SSN			
Credit/Debit Card/Financial Data			
Health Information			
Biometric Data			
Geolocation Data			
Other Sensitive Personal Data			
CPNI			
Account #			
Telephone #			
Call Data			
Internet Protocol Detail			
Type of Service			

Subscriber Bill			
Others			