DATA PRIVACY ADDENDUM FOR VENDORS AND THIRD-PARTY REPRESENTATIVES

This Brightspeed 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 Connect Holding II LLC d/b/a Brightspeed or the Brightspeed Affiliate identified in the Agreement ("**Brightspeed**") and the vendor, service provider, contractor, third-party representative, or Representative ("**Representative**" or "**Supplier**") indicated in the applicable Agreement and is effective as of the effective date of the Agreement. Brightspeed 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. Brightspeed "Affiliates" are limited to subsidiaries under the direct and indirect Control of Brightspeed.

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 Brightspeed; 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 Representative 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 "**Representative Personnel**" means (a) all employees, agents, contractors and/or subcontractors of Representative, 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 Representative's Subprocessors.

1.10. "**Provided Services**" means any and all products or services provided by Representative to Brightspeed 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 Brightspeed's services; or (c) unauthorized access or modification to Brightspeed's systems or systems used to access, process, or store Brightspeed Data or Brightspeed's systems or networks.

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

1.16. "**U.S. Records**" means Brightspeed'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 Brightspeed 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 Representative's Processing of Personal Data, Brightspeed is the "Controller", and Representative 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.** Representative will comply with Data Privacy Laws and protect Personal Data as required by Data Privacy Laws and this DPA. Brightspeed has the right to take reasonable and appropriate steps to help ensure that Representative uses Personal Data in a manner consistent with Brightspeed's obligations under Data Privacy Laws. If Representative reasonably determines that it is unable to meet its obligations under Data Privacy Laws and this DPA, Representative will notify Brightspeed without undue delay. Brightspeed 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 Representative to suspend its Processing of Personal Data. Any such suspension will continue until Representative can meet its obligations under Data Privacy Laws and this DPA. However, if, in Brightspeed's sole determination, Representative cannot meet its obligations under Data Privacy Laws and this DPA within a reasonable amount of time, Brightspeed may terminate the Agreement for Representative's breach of this DPA. This breach and termination of the Agreement will be without penalty, additional cost, and liability to Brightspeed, and without limiting Brightspeed's remedies at equity and law, Representative shall promptly refund any unused, prepaid fees.

5. **Confidentiality.** Personal Data shall be considered Brightspeed's Confidential Information. Representative shall hold Personal Data in strict confidence. Representative will not disclose Personal Data to any third party, including Representative's Affiliates, unless such disclosure is expressly permitted under the Agreement. Representative 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, Representative shall: (a) limit access to Personal Data only to those entities and individuals, including Representative'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 Brightspeed; (b) ensure that Representative 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 Representative.

6. **Data Transfer.** Representative 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 Brightspeed's prior written approval.

7. **Security Measures.** Without limiting any data security provisions in the Agreement, Supplier will implement and maintain industry best practices physical, administrative, and technical safeguards that protect the confidentiality, integrity, availability, and security of Brightspeed Data, Brightspeed's systems and, networks, and of Representative's systems and networks with access to Brightspeed Data and are designed to prevent Security Incidents (the "**Security Measures**"). Such Security Measures shall: (a) be at least as protective as the measures Representative 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 Brightspeed Security Addendum.

8. **Security Incident and Response.**
   8.1. Security Incident Response Plan. Representative shall implement and maintain an Incident Response Plan that enables Representative 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 Brightspeed Data.
   8.2. Notification of Security Incident. In the event of a Security Incident, Representative shall notify Brightspeed without undue delay, and in no event later than forty-eight (48) hours after the initial detection of a Security Incident by contacting Brightspeed's Cyber Incident Response Team at cirt@brightspeed.com. Such notification shall include all information necessary for Brightspeed 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 Representative that Brightspeed may contact to obtain further information and updates.
   8.3. Response to Security Incident. At Representative's sole expense, Representative 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 Brightspeed with all information, logs, or images reasonably requested by Brightspeed in connection with the Security Incident, including, but not limited to, all information to allow Brightspeed and each Brightspeed Affiliate to meet any obligations to report or inform of the Security Incident under Data Privacy Laws and assess the risk to Brightspeed, or Brightspeed Data, including Personal Data. Representative will promptly provide Brightspeed with updated notifications as it becomes aware of additional material information and regularly keep Brightspeed apprised of the status of the Security Incident and all matters related to it.
   8.4. Cooperation. Representative shall cooperate with Brightspeed'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. Representative acknowledges and agrees that it is Brightspeed's decision whether and when to disclose a Security Incident to affected individuals or regulators in the absence of any laws or regulations requiring Representative to report or notify.
   8.6. Public Statements. Representative shall not make any public statement about any Security Incident or Brightspeed security vulnerability nor notify affected individuals of any Security Incident without Brightspeed's prior written approval, unless Representative is required to do so pursuant to applicable Laws, in which case it shall provide Brightspeed 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 Representative or by any Representative Personnel of the representations, warranties or covenants contained in this Security Addendum; (b) any Information Security Incident; or (c) breach or alleged breach of Representative's obligations under this Security Addendum relating to privacy or security or caused by Representative's negligence or willful misconduct, Representative shall pay for or reimburse Brightspeed for (i) expenses incurred to provide warning or notice to Brightspeed'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 Brightspeed; (ii) expenses incurred either directly by Brightspeed or through Brightspeed'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 Brightspeed's regulators or any other similar protective measures designed to mitigate any damages to the Affected Persons; (iv) fines, penalties, or interest that Brightspeed 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 Brightspeed related to any Security Incident.
respond to the Security Incident in accordance with the Security Incident and Response requirements of the Security Addendum.

9. Representative's Assistance with Brightspeed's Compliance. Representative shall implement appropriate technical and organisational measures and other assistance reasonably necessary for Brightspeed 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. Brightspeed may take appropriate steps to ensure that Representative Processes Personal Data in a way that is consistent with Brightspeed's obligations under Data Privacy Laws and Representative shall cooperate and assist Brightspeed with such efforts. In the event of an investigation related to Representative's Processing of Personal Data, Representative will provide all assistance and support related to said investigation.

10. Data Processing. Representative 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 Brightspeed, except where otherwise required by law. Representative will provide prompt notice to Brightspeed in the event Representative believes Brightspeed's instructions violate Data Privacy Laws. The parties further acknowledge and agree that: (a) Brightspeed's disclosure of Personal Data to Representative hereunder does not constitute a Sale and (b) Personal Data disclosed by Brightspeed to Representative is provided to Representative only for the limited and specified purposes set forth in the Agreement and this DPA.

11. Processing Restrictions. Representative will not access, collect, retain, use, disclose, or otherwise Process Personal Data (a) outside the direct business relationship with Brightspeed; or (b) for any purpose other than performing the Processing in accordance with this DPA and the Agreement. Representative will not rent, lease, or Sell Personal Data, or share it for targeted online advertising. Representative will not combine Personal Data with data received from or on behalf of any third party or collected by or on behalf of Representative, 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, Representative will obtain Brightspeed's approval as follows: (i) notify Brightspeed 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 Brightspeed to find a replacement.

12.2. **Subprocessors.** Representative shall not disclose any Personal Data to any Subprocessor unless authorized by Brightspeed. Authorized Subprocessors may be attached hereto as Annex B. Representative shall notify Brightspeed 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. Brightspeed may object to the proposed Subprocessor by providing Representative written notice of such objection. Upon receiving such an objection, Representative shall: (a) work with Brightspeed 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 Brightspeed in its objection. If Representative informs Brightspeed that such change or corrective steps cannot be made, Brightspeed may immediately terminate all or a portion of the Agreement for convenience and receive a refund of any prepaid fees. Representative 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 Representative with respect to Personal Data. Representative shall be liable for all acts and omissions of the Subprocessor as if they were Representative's acts and omissions.

13. Individual Rights Requests.

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

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

14. Records and Audits. Representative 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 Representative, Representative shall permit Brightspeed, its auditors, designated representative and regulators, to audit and inspect, at Brightspeed'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 Representative's facilities where Personal Data is stored or maintained by or on behalf of Representative; (b) any computerized or paper systems used to share, disseminate, or otherwise Process Personal Data; (c) Representative's security practices and procedures related to Processing Personal Data; and (d) records required to be retained by Representative under this DPA, the Agreement, or applicable Laws.

15. Security Assessments. Brightspeed may perform periodic security assessments, which may include assessment of certain portions of the systems involved in Processing Personal Data. Representative agrees to cooperate with, contribute to, and provide Brightspeed with all information necessary to demonstrate the Representative's compliance with this DPA and Data Privacy Laws, at Representative's expense. Representative and Brightspeed

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, Representative will securely return or delete all Personal Data, as Brightspeed chooses, except to the extent Representative is expressly required by law to retain such Personal Data. Representative will notify Brightspeed in writing when the data has been deleted, if Brightspeed chooses deletion. If Representative is legally required to retain Personal Data, Representative will provide Brightspeed 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 Representative will apply to the Personal Data. Representative will securely return or delete the Personal Data, at Brightspeed's option, when the legal justification for retaining the Personal Data no longer applies. Representative 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 Representative'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, Representative shall indemnify and hold harmless Brightspeed and Brightspeed'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 Representative'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 Brightspeed (or any of Brightspeed's Affiliates, employees, or agents) is or may be entitled to indemnification under this DPA, Brightspeed may, at Brightspeed's option, require Representative to defend such Claim at Representative's sole expense. Representative shall not settle any such Claim without Brightspeed'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 cirt@brightspeed.com using the subject line: Security Breach.
    20.2. Other notifications related to this DPA should be sent to privacy@brightspeed.com using the subject line: Brightspeed 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, any other document comprised within the Agreement, and the Brightspeed Supplier Portal, 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, 5) the Supplier Portal, and 6) 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 begins on the Effective Date of the Agreement and will end upon the later of (a) termination of the Agreement; or (b) Representative's destruction or return of all Personal Data Processed by Representative 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.

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

Annex A1: Details of Processing of Personal Data for Third-Party Representatives (Parties to the Master Representative Agreement ("MRA"))

Annex A2: Details of Processing of Personal Data for other Vendors (Parties to all other forms of the Agreement, excluding the MRA)

Annex A1: Details of Processing of Personal Data for Third-Party Representatives
(Parties to the Master Representative Agreement ("MRA"))

Processor Details
Please provide contact details for processor.

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

Applicable Data Subject or data element categories.

	Customers, only when the FCC Addendum applies per the terms of the Agreement	**Employees**	**Potential Customers and Others**
Personal Identifiers			
Name	X		X
Email	X		X
Street Address	X		X
Existing Phone Number	X		X
Account #	X		
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 #	X		
Telephone #	X		
Call Data	X		

Internet Protocol Detail			
Type of Service	X		
Subscriber Bill	X		
Others			

Annex A2: Details of Processing of Personal Data for other Vendors
(Parties to all other forms of the Agreement, excluding the MRA)

Processor Details
Please provide contact details for processor.

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