

**EXHIBIT D**  
**DATA PROTECTION ADDENDUM**

This Data Protection Addendum (“Addendum”) is attached to and made a part of the Master Agreement between Supplier and CenturyLink dated \_\_\_\_\_.

1. Definitions.

- a. “Agreement” shall mean any agreement to which Supplier and CenturyLink are parties and pursuant to which Supplier Processes any CenturyLink Personal Data or Personal Information, whether acting as a licensor or service provider to CenturyLink, authorizing CenturyLink to resell certain Supplier products, or any other relationship between the parties.
- b. “Data Protection Laws” means all applicable laws, regulations and regulatory guidance in relation to the Processing and protection of Personal Data including but not limited to the European Union’s , General Data Protection Regulation (“GDPR”), the California Consumer Privacy Act (“CCPA”) or any other relevant Data Protection Law.
- c. “Personal Data” or “Personal Information” has the meaning set forth in the relevant Data Protection Law.
- d. “Process” or “Processing” means direct or indirect receipt, access, storage, disclosure, dissemination, transmission, or use of any Personal Data or the meaning set specifically forth in the relevant Data Protection Law.
- e. Any reference to “Supplier” herein means Supplier or Service Provider and any of its affiliates, agents, or representatives who may Process any Personal Data, or any Sub-Processors, whether or not any such parties are referred to in the relevant clause, on behalf of CenturyLink.
- f. All other terms used herein shall have the meaning set forth in the relevant Data Protection Law, or as specified elsewhere in the Agreement(s).

2. Compliance with Laws. Supplier guarantees it will implement appropriate technical and organizational measures in such a manner that Processing under this Addendum will meet the requirements under the Data Protection Laws.

3. Restriction on Sub-Processors.

- a. Subject to the terms of this Addendum and any terms in an Agreement regarding the use of subcontractors, CenturyLink authorizes Supplier to engage other parties for Processing Personal Data (each such party, a “Sub-Processor”) on behalf of CenturyLink. Supplier shall maintain a list of all Sub-Processors engaged by Supplier and provide CenturyLink with a copy of such list upon request. In the event Supplier changes any Sub-Processor, whether by addition or replacement, Supplier shall provide CenturyLink with prior written notice of any such changes. CenturyLink shall have thirty (30) days to object to any such change.
- b. Notwithstanding the foregoing, Supplier shall only engage such Sub-Processor for carrying out the specific Processing activities authorized by CenturyLink pursuant to the terms of a written agreement containing the same obligations as set out herein with respect to such Sub-Processor’s Processing of Personal Data. In the event any Sub-Processor fails to fulfil its obligations under such written agreement, Supplier shall remain fully liable to CenturyLink for the performance of such Sub-Processor’s obligations.

4. Personal Data Processing.

- a. In the event Supplier Processes Personal Data on behalf of CenturyLink, the duration, nature and purpose of the Processing for specific services, along with the type of Personal Data and categories of Data Subjects, shall be documented separately in Statements of Work, Order Forms, and similar attachments to the Agreements.
- b. Supplier shall only Process Personal Data on CenturyLink's documented instructions. If Supplier believes that CenturyLink's instructions violate or are likely to violate applicable law, Supplier shall immediately notify CenturyLink of the same. Supplier shall not engage in any Processing until the parties have resolved the legality of the Processing. In the event Supplier is required to Process Personal Data for a reason other than as instructed pursuant to applicable law to which the Supplier is subject, prior to any such engaging in any additional Processing, Supplier shall inform CenturyLink of that legal requirement, unless the applicable law prohibits such disclosure.
- c. Supplier shall ensure that persons authorized to Process Personal Data are subject to appropriate confidentiality requirements.
- d. At CenturyLink's option, Supplier shall permanently destroy or return all Personal Data to CenturyLink after the end of the provision of services relating to Processing of such Personal Data and shall permanently destroy all existing copies of such Personal Data in accordance with the terms set forth herein unless applicable law requires Supplier to maintain the Personal Data. In the event Supplier retains Personal Data pursuant to legal requirements, Supplier shall (i) provide CenturyLink with written notice of such requirements; (ii) continue to protect such retained Personal Data in accordance with this Addendum; and (iii) only use such retained Personal Data to fulfil Supplier's obligations under such legal requirements. Proper destruction methods include those widely recognized in the industry as sufficiently rendering retrieval, restoration, or reconstruction of any Personal Data practicably impossible, regardless of the form or media. Upon CenturyLink's request, Supplier shall cause an executive officer of Supplier to formally certify, in form and content reasonably satisfactory to CenturyLink, to Supplier's compliance with the foregoing destruction requirements.
- e. Supplier shall, to the extent possible given the nature of the Processing, fully assist CenturyLink with its obligation to respond to an individual's request to exercise the rights afforded them under the relevant Data Protection Law.
- f. Supplier shall maintain a written record of all categories of Processing activities carried out on behalf of CenturyLink. At a minimum, such written record shall contain:
  - i. The name and contact details of Supplier's personnel that are competent to respond to inquiries about Supplier's Processing activities and, if applicable, Supplier's Data Protection Officer;
  - ii. The name and contact details for any Sub-Processor Processing Personal Data on behalf of CenturyLink in accordance with the terms of this Addendum and, if applicable, such Sub-Processor's Data Protection Officer;
  - iii. The categories of Processing carried out on behalf of CenturyLink;
  - iv. Where applicable, information about transfers of Personal Data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers to a country that does not provide adequate

protection for Personal Data within the meaning of Article 45 of the GDPR, documentation of the suitable safeguards implemented to enable such transfer; and

- v. Where possible, a general description of the technical and organizational security measures referred to in Section 5.

Supplier shall make a copy of the record available to CenturyLink and/or to any supervisory authority upon request.

- g. In the event CenturyLink determines, in its sole discretion, that a data protection impact assessment is required under Article 35 of the GDPR for Processing undertaken by Supplier, Supplier shall fully cooperate with CenturyLink to enable CenturyLink to complete any such data protection impact assessment, which may include, without limitation:
  - i. Developing a systematic description of the Processing operations and the purposes of the Processing;
  - ii. Conducting an assessment of the necessity and proportionality of the Processing operations in relation to the purposes;
  - iii. Conducting an assessment of the risks to the rights and freedoms of Data Subjects with respect to the Processing; and
  - iv. Documenting the measures envisaged and/or employed to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with this Addendum and the Data Protection Laws.
- h. Supplier and, where applicable, its representatives and Sub-Processors, shall cooperate, on request, with any governing body's performance of its tasks mandated under the relevant Data Protection Law.
- i. Under the requirements of the GDPR, Supplier shall not transfer any Personal Data to any third country or international organization without the written consent of CenturyLink. In the event CenturyLink consents to Supplier's transfer of any Personal Data to a third country or international organization, CenturyLink's consent to such transfer shall be conditioned on the existence of one of the following circumstances:
  - i. The transfer is to a country that is a member of the EU;
  - ii. The transfer is to a country, or a territory or specified sector within such country that is deemed to provide an adequate level of protection for Personal Data in accordance with Article 45 of the GDPR;
  - iii. The transfer is subject to appropriate safeguards, including the condition that enforceable Data Subject rights and effective legal remedies for Data Subject are available in accordance with Article 46 of the GDPR; or
  - iv. The purpose of the transfer falls within one of the specified situations set forth in Article 49 of the GDPR; provided, however, Supplier shall not transfer any Personal Data under this Section 4.j.iv without CenturyLink's prior written consent.

Supplier shall maintain a written record of all transfers to third countries or international organizations made pursuant to this Section and shall make a copy of such record available to CenturyLink and/or any supervisory authority upon request. If requested by CenturyLink, Supplier agrees to execute a separate international data transfer agreement. The international data

transfer agreement will incorporate the rights and obligations of the parties set forth herein as well as any specification necessary to comply with Data Protection Laws.

5. Information Security Measures. In addition to, and not in lieu of, any information security requirements set forth in the Agreements, Supplier shall implement appropriate technical, administrative and organizational measures to ensure that Personal Data is protected against accidental or unlawful Processing, destruction, loss, alteration, unauthorized disclosure of, or access to such Personal Data, and such measures to the extent appropriate under the circumstances and taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing shall include but not limited to the requirements of the Information Security and Privacy Requirements found here: <https://www.CenturyLink.com/en-us/about/doing-business-with-CenturyLink.html>, as well as:
  - a. Pseudonymizing and/or encrypting Personal Data;
  - b. Reasonable steps to ensure reliability and integrity of any Supplier personnel or permitted Sub-Processor who have access to Personal Data and appropriate measures to ensure that such parties are informed of the confidential nature of Personal Data and comply with the obligations set forth in this Addendum;
  - c. Testing, assessing and evaluating the effectiveness of information systems for ensuring the security of Processing;
  - d. Reasonable steps to ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
  - e. Reasonable steps to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services utilized to Process Personal Data.
6. Right to Audit; Requirement to Provide Compliance Records.
  - a. Supplier shall permit CenturyLink, or its duly authorized representatives, on reasonable prior notice, to inspect and/or audit the Supplier's (and Supplier's Sub-Processors') Processing activities that are relevant to the Processing of Personal Data, to verify that Supplier's (and its Sub-Processors') Processing activities related to Personal Data are in compliance with this Addendum, CenturyLink's instructions and Data Protection Laws. Supplier shall make available to CenturyLink all information reasonably necessary to demonstrate Supplier's compliance with its obligations as set forth in this Addendum and allow for and contribute to audits and inspections conducted by CenturyLink. CenturyLink's audit rights herein may include audits and inspections of any Supplier activities, systems, materials, policies, records, information security programs and facilities involved in Processing any CenturyLink Personal Data.
  - b. In addition to the foregoing requirement to provide information and assistance in relation to an audit conducted pursuant to Section 6.a, Supplier shall maintain a written record of all information necessary to demonstrate its compliance with the obligations set forth in this Addendum. Supplier shall provide a copy of such record to CenturyLink upon request.
7. Data Breach. In the event of Supplier becomes aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Supplier (a "Data Breach"), Supplier shall notify CenturyLink of such Data Breach without undue delay (and in no event more than twenty-four (24) hours of becoming aware of any such Data Breach) and of any facts known to Supplier regarding the Data Breach, and cooperate fully with CenturyLink in order to mitigate and remediate the Data Breach. Supplier shall be deemed to be aware of a Data Breach when Supplier

has a reasonable degree of certainty that a Data Breach has occurred that has led to Personal Data being compromised. At a minimum and where available, the notification of a Data Breach shall include the following:

- a. Description of the nature of the Data Breach including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
- b. The name and contact details of Supplier's Data Protection Officer, if applicable, or other contact point where additional information can be obtained;
- c. Description of the likely consequences of the Data Breach; and
- d. Description of the measures taken or proposed to be taken by Supplier to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

In the event Supplier does not have all of the information referenced above at the time it provides its initial notification to CenturyLink of a Data Breach, Supplier shall continue to investigate such Data Breach and provide the above-referenced information as it becomes available.

8. CCPA. As required by the CCPA, Supplier certifies that it has read and understands the applicable requirements of the California Consumer Privacy Act, AB 375 ("CCPA"). The parties acknowledge that Supplier is a Service Provider as defined therein. Accordingly, Supplier will not: (i) sell the personal information disclosed to it by CenturyLink; (ii) collect, retain, use, or disclose the personal information disclosed to it by CenturyLink for any purpose other than providing the Services, outside of the direct business relationship between the parties, or as otherwise permitted by the CCPA; and (iii) further collect, sell, or use the personal information disclosed to it by CenturyLink except as necessary to perform the business purpose for which Supplier was retained.
9. Indemnification. Supplier shall defend, indemnify and hold harmless CenturyLink from and against any and all claims, suits, liabilities, expenses, attorney's fees or damages arising as a result of claims related to Processing or protection of Personal Data within the Supplier's control or Supplier's alleged or actual breach of the terms of this Addendum.
10. No Limitation of Liability. Notwithstanding anything to the contrary in any Agreement, any and all limitations of liability or other caps on damages set forth in any Agreement shall not apply to any damages arising out of or relating to Supplier's breach of the terms of this Addendum.
11. Interpretation with Agreement(s). This Addendum is intended to supplement the Agreement between the parties and not replace existing obligations. This Addendum is subject to the terms and conditions of the Agreement and shall be deemed part of the Agreement. In the event of a conflict between the Agreement and this Addendum, this Addendum shall prevail; provided, however, if such conflict arises as a result of multiple obligations with respect to security or privacy, the stricter obligation shall apply. Supplier's failure to comply with any of the provisions of this Addendum shall be deemed a material breach of the Agreement.