

## DATA PROTECTION ADDENDUM

This Data Protection Addendum, including its Appendices, (the “**DPA**”) forms part of, amends, and supplements the Communication Services Agreement, the Reseller Services Agreement, the Terms of Services, and/or any other written agreement entered into between the Parties that covers the use of the Services, as applicable (the “**Services Agreement**”) by and between Bandwidth Inc. and/or its Affiliates (“**Bandwidth**”) and Customer for the purchase of Services from Bandwidth to reflect the parties’ agreement with regard to the Processing of Personal Data effective December 27, 2022. Both Bandwidth and Customer may also be referred to as “**Party**,” or may collectively be referred to as the “**Parties**.”

### Section 1. Definitions.

- Any capitalized term used in this DPA that is not defined herein will have the meaning set forth in the Services Agreement.
- “**Affiliate**” means in relation to a Party, any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. For purposes of this definition, “control” means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
- “**Bandwidth Privacy Notice**” means Bandwidth’s current Privacy Notice available at: <https://www.bandwidth.com/privacy/>.
- “**Communications Content**” means any information exchanged or conveyed between end users via the Services, such as content of calls, faxes, and messages sent or received via the Services.
- “**Communications Metadata**” means information generated in connection with the conveyance of communications via the Services, such as source and destination information, IP address, time duration or completion status.
- “**Controller**” will have the following meanings: (a) “controller” as set forth in the GDPR; (b) “business” as set forth under the CCPA; and (c) “controller” as set forth under any other U.S. Privacy Laws.
- “**Customer Account Information**” means: (i) information used for Customer’s account billing and payment or to prevent fraud or misuse of the Services such as: name, email address, phone number of a Customer’s representative; and (ii) other information Bandwidth may Process in the context of creating or maintaining a business relationship with Customer for purposes of the Services.
- “**Data Protection Laws**” means all data protection and privacy laws and regulations applicable to either Party’s Processing of Personal Data and the provision of electronic communications under the Services Agreement, including but not limited to, European Union (EU), European Economic Area (EEA) Member States laws and regulations with respect to Personal Data and privacy of electronic communications, and any other applicable data protection or privacy laws and regulations of any other country or state, including U.S. Privacy Laws.
- “**Data Subject**” means a natural person about whom data is provided to Bandwidth pursuant to this DPA, including those listed at Appendices 1 & 2.
- “**EU Standard Contractual Clauses**” means the standard contractual clauses adopted by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, or any subsequent version thereof released by the European Commission. In the event any subsequent version of such clauses is released that is applicable to the Services, the parties agree that the then-current version of the clauses will apply, in which case any references in this DPA to specific clauses shall be deemed to refer to equivalent clauses in the then-current version of the clauses, regardless of their enumeration.
- “**General Data Protection Regulation**” (or “**GDPR**”) means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC and all applicable EU and European Economic Area (EEA) Member State legislation implementing the same.
- “**Personal Data**” means any information relating to an identified or identifiable natural person, directly or indirectly, and includes similarly defined terms in Data Protection Laws, including, but not limited to, “personal data” and “personal information.”
- “**Process**” or “**Processing**” will have the meaning set forth under Data Protection Laws.
- “**Processor**” will have the following meanings: (a) “processor” as set forth in the GDPR; (b) “service provider” as set forth under the CCPA; (c) “processor” as set forth under any other U.S. Privacy Laws; and (d) “processor” or materially equivalent term as set forth in other Data Protection Laws.
- “**Security Incident**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure, acquisition, or access to, Personal Data transmitted, stored or otherwise Processed.

- **“Services”** will have the same meaning as in the Services Agreement, which may include the Processor Services as defined in Section 2.2.
- **“Subprocessor”** means any third party engaged by Bandwidth to Process Personal Data on Customer’s behalf in connection with the Processor Services.
- **“Subscriber Data”** means any identifying information about Subscribers or End Users that Bandwidth may collect from Customer to comply with local regulatory requirements or provision of Services, such as name, birth date, physical address, nationality, or identification card of the appointed representative of Subscriber. For purposes of this DPA, “Subscriber Data” includes “End User Information” and “Location Information” as those terms may be used in the Services Agreement.
- **“Supervisory Authority”** will have the following meanings: (a) Supervisory Authority as set forth under the GDPR; and (b) a state regulatory agency with authority to enforce U.S. Privacy Laws.
- **“U.K. Addendum”** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner’s Office under S119A(1) Data Protection Act 2018, Version B1.0 in force 21 March 2022.
- **“U.S. Privacy Laws”** means all U.S. laws, rules, regulations, directives, and government requirements and guidance, federal or state, currently in effect and as they become effective relating in any way to privacy, confidentiality, security or consumer protection that are applicable to Personal Data. U.S. Privacy Laws includes, but is not limited to, the California Consumer Privacy Act as amended by the California Privacy Rights Act (CPRA), Cal. Civ. Code 1798.100 et seq. and any regulations and guidance that may be issued thereunder (“CCPA”), the Consumer Data Protection Act, Code of Virginia Title 59.1 Chapter 52 § 59.1-571 et seq., the Colorado Privacy Act, Colorado Revised Statute Title 6 Article 1 Part 13 § 6-1-1301 et seq., the Act Concerning Personal Data Privacy and Online Monitoring, Connecticut Public Act No. 22-15, and the Consumer Privacy Act, Utah Code Annotated Title 13 Section 2 § 1 et seq.

## **Section 2. Roles of the Parties.**

**2.1 Independent Controllers.** Bandwidth acts as an independent Controller, and Customer as an independent controller, with respect to Personal Data contained in Customer Account Information, Communications Metadata, and Subscriber Data, and in any other instances pursuant to the Services Agreement where Bandwidth acts as a Controller, as determined by applicable Data Protection Laws.

**2.2 Processor.** In limited circumstances, Bandwidth may act as a Processor on behalf of Customer as Controller; for example, where Customer has subscribed to specific add-on Services to enable Processing of Communications Content or Communications Metadata at the Customer’s instructions, and in any other instances pursuant to the Services Agreement where Bandwidth acts as a Processor, as determined by applicable Data Protection Laws (“**Processor Services**”). To the extent applicable, Customer appoints and authorizes Bandwidth to act as Processor on Customer’s behalf, and Bandwidth will process such Personal Data in accordance with Customer’s instructions as set forth in Section 4.

## **Section 3. Independent Controllers.**

**3.1 Bandwidth as Independent Controller.** Bandwidth will Process Customer Account Information, Communications Metadata, and Subscriber Data as an independent Controller to provide the Services in accordance with this DPA and in accordance with Data Protection Laws, applicable telecommunications laws and regulations, the Services Agreement, and the Bandwidth Privacy Notice. For example, Bandwidth will Process (i) Communications Metadata to provide, maintain, bill and optimize its Services and to prevent fraud or misuses of the Services and comply with local regulatory requirements; (ii) Customer Account Information for billing and payment, to prevent fraud or misuse of the Services, and to maintain or manage a business relationship with Customer; and (iii) Subscriber Data to comply with local regulatory requirements and provision of the Services (e.g., telephone number assignments, number portability, or provision of emergency services).

**3.2 Customer as Independent Controller.** Customer, as an independent Controller, will ensure that its Processing of Personal Data complies with Data Protection Laws, including, to the extent applicable, by ensuring that Customer has provided prior notice and obtained consent for such Processing related to the Services. For illustration, and without limiting the foregoing, Customer may collect Subscriber Data that may need to be transmitted to Bandwidth in order for Bandwidth to provide the Services to Customer and in such case Customer will ensure that prior notice has been provided to the Subscriber with respect to the Processing and its purpose(s) and, where required, that the Subscriber has given his or her consent unambiguously for the Processing of such data.

**3.3 Data Subjects’ Rights.** The Parties agree that, in the event of receiving from a Data Subject a complaint or a request to access their Personal Data that may involve the other Party, the Party receiving such a request will notify the other Party without undue delay, and will provide such cooperation and assistance as may reasonably be required to enable that Party to respond to any such complaint or request in accordance with the provisions of applicable Data Protection Laws.

**3.4 Storage and Deletion.** Bandwidth will store Personal Data Processed in the course of the provision of the Services for so long as it is needed for the provision of the Services and/or for compliance with local regulatory requirements, in accordance with Data Protection Laws and any other applicable laws.

## Section 4. Processor Obligations.

**4.1 Bandwidth as Processor.** The terms of this Section 4 apply where and to the extent Bandwidth provides Processor Services to Customer. In such a situation, Bandwidth will Process the Personal Data only (i) on behalf of Customer; (ii) in accordance with the Services Agreement and/or DPA (including the details of Processing in Appendix 2.B) as necessary to provide the Processor Services to Customer; and (iii) for the purpose of fulfillment of Customer's documented reasonable instructions, where such instructions are consistent with the terms of the Services Agreement. Bandwidth will follow such instructions, unless in Bandwidth's opinion an instruction infringes Data Protection Laws, in which case Bandwidth will inform Customer immediately. Bandwidth will not otherwise access or use the Personal Data, except as necessary to maintain or provide the Services in accordance with industry standards or as necessary to comply with applicable law or other binding governmental requirement or order.

**4.2 U.S. Provisions.** For purposes of U.S. Privacy Laws, Bandwidth agrees it will not (i) "sell" or "share" (as that term is defined in the CCPA) Personal Data; (ii) retain, use, or disclose Personal Data for any purpose other than for the specific purpose of performing functions under the Services Agreement and under this DPA, including retaining, using, or disclosing Personal Data for a commercial purpose other than performing functions under the Services Agreement and this DPA or retaining Personal Data subsequent to the termination of the Services Agreement; (iii) retain, use, or disclose Personal Data outside of the direct business relationship between Bandwidth and Customer; or (iv) with respect to Personal Data subject to the CCPA, combine Personal Data received in connection with performing functions under the Services Agreement and under this DPA with Personal Data it receives from another source except to perform Business Purposes (as defined by and specified in the CCPA). Notwithstanding the foregoing, Customer agrees that Bandwidth may, if otherwise permitted by U.S. Privacy Laws and subject to Bandwidth's confidentiality obligations hereunder, Process Personal Data to the extent permitted or required by applicable law, including to perform other Processing functions permitted by U.S. Privacy Laws. In connection with providing the Services, Bandwidth will also (i) comply with the CCPA and provide the same level of privacy protection as is required by the CCPA for Personal Data; (ii) allow Customer to take reasonable and appropriate steps to help ensure that Bandwidth uses Personal Data in a manner consistent with Customer's obligations under the CCPA; (iii) notify Customer promptly in writing if it makes a determination that it can no longer meet its obligations under the CCPA; and (iv) permit Customer to, upon notice, take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data. Bandwidth understands the restrictions set forth in this Section and will comply with them.

**4.3 Subprocessors.** Bandwidth's Subprocessor list is available at <https://www.bandwidth.com/legal/bandwidth-subprocessors/>. Customer authorizes Bandwidth to engage Subprocessors in connection with the performance of the Processor Services, provided that: (i) Bandwidth has entered into a written agreement with each Subprocessor containing data protection obligations not less protective than those set forth in this DPA as applicable to the nature of the Processor Services provided by such Subprocessor; (ii) Bandwidth remains liable for Subprocessor's compliance with the obligations in this DPA; and (iii) Bandwidth will provide email notice to Customer prior to Bandwidth's appointment of a new Subprocessor and Customer may object to such appointment, provided such objection is submitted to Bandwidth in writing within ten (10) business days after receipt of Bandwidth's email notice and is based on reasonable grounds relating to data protection and privacy. In the event of such objection by Customer, the Parties will discuss commercially reasonable alternative solutions in good faith. If the Parties cannot promptly reach resolution and Bandwidth elects to appoint the Subprocessor, Customer may suspend or terminate the Services Agreement as its sole and exclusive remedy. Customer is responsible for all fees, charges, or taxes incurred by Customer prior to suspension or termination.

**4.4 Assistance with Data Subjects' Requests.** Bandwidth will provide reasonable assistance to Customer to comply with Data Protection Laws, including reasonable assistance related to Data Subject Requests in connection with the Processor Services. Bandwidth will, to the extent legally permitted, notify Customer if Bandwidth receives a request from a Data Subject in connection with the Processor Services that (i) identifies Customer, (ii) relates to Personal Data, and (iii) seeks to exercise the Data Subject's rights (each a "Data Subject Request"). Notwithstanding the foregoing, Customer acknowledges and agrees that Bandwidth may not have the ability to match Communications Content and/or Communications Metadata with a Data Subject name, in which case, Bandwidth will inform Customer or the Data Subject, as appropriate, accordingly. In such a case, Customer agrees that Bandwidth is not in a position to identify the Data Subject, and therefore Bandwidth is exempt from fulfilling its obligation to provide further assistance to Customer with respect to the Data Subject Request. If at any time Bandwidth can no longer meet its obligations under Data Protection Laws, it will provide Customer notice thereof.

**4.5 Assistance with Data Protection Impact Assessments.** Where appropriate in its discretion Bandwidth will provide reasonable assistance and necessary information to Customer, at Customer's expense, in the preparation of Customer's data protection impact assessments and, where necessary, carrying out consultations with any Supervisory Authority that may be required in accordance with Data Protection Laws.

**4.6 Deletion.** Following termination or expiration of the Services Agreement, Bandwidth will delete any Personal Data (if any is in its possession) Processed in connection with the Processor Services and for which Customer serves as a Controller. Notwithstanding anything in this Section, Bandwidth will retain Personal Data, or any portion of it, that may be required by applicable law.

## Section 5. Audits.

**5.1 Reports.** Bandwidth uses external auditors to verify the adequacy of its security measures with respect to its processing of Personal Data. Such audits are conducted at least annually, are performed at Bandwidth's expense by independent third-party security professionals at Bandwidth's selection, and result in the generation of a confidential audit report ("Report"). Bandwidth

will provide a list of Bandwidth's relevant certifications and/or standards to Customer promptly upon Customer's request to [privacy@bandwidth.com](mailto:privacy@bandwidth.com). Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Bandwidth will make available to Customer a copy of Bandwidth's most recent Report.

**5.2 Audits.** The parties acknowledge that Customer must be able to assess Bandwidth's compliance with its obligations under applicable Data Protection Laws and this DPA, insofar as Bandwidth is acting as a Processor on behalf of Customer. If the Report does not provide, in Customer's reasonable judgment, sufficient information to confirm Bandwidth's compliance with the terms of this DPA, then Customer or an accredited third-party audit firm agreed to by both Customer and Bandwidth (or, with respect to Bandwidth's role as Processor, a third party mandated by Customer as Controller in accordance with Article 28 of the GDPR) may audit Bandwidth's compliance with the terms of this DPA during regular business hours, with reasonable advance notice to Bandwidth, and subject to reasonable confidentiality procedures. Customer is responsible for all costs and fees related to such audit. Customer will promptly notify Bandwidth with information regarding any non-compliance discovered during the course of the audit. Customer may not audit Bandwidth more than once annually.

## **Section 6. Security and Confidentiality.**

**6.1 Security Measures.** Bandwidth will maintain appropriate technical and organizational measures to protect the security, confidentiality, and integrity of Personal Data Processed in the course of the provision of the Services from a Security Incident. At a minimum, Bandwidth will provide at least the same level of privacy protection as required by Data Protection Laws and will ensure the security measures specified in **Appendix 3** (the "**Security Measures**"). Customer has assessed the Security Measures and agrees that the Security Measures provide an appropriate level of security for the Personal Data, taking into account the risks presented by the Processing. Bandwidth may, from time to time, modify the Security Measures, provided, however, that the Security Measures as modified will not reduce the level of protection provided for Personal Data.

**6.2 Security Incidents.** In the event of a Security Incident concerning Personal Data Processed by either Party as an independent Controller, the Party experiencing the Security Incident will be solely responsible for taking appropriate measures to address the Security Incident, including measures to mitigate its possible adverse effects. If Bandwidth becomes aware of a confirmed Security Incident containing the Personal Data of Data Subjects, for categories of data for which Bandwidth acts a Processor, Bandwidth will notify Customer of the Security Incident promptly after becoming aware, via [security@bandwidth.com](mailto:security@bandwidth.com), and will provide commercially reasonable support to Customer in the context of its obligations according to applicable Data Protection Laws and to the extent it is within Bandwidth's control. Bandwidth's notification of the Security Incident will include, to the extent known at the time of notification, (i) a description of the Security Incident, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned, (ii) the name and contact details of Bandwidth's data protection officer or other contact point where more information can be obtained, (iii) a description of the likely consequences of the Security Incident, and (iv) a description of the measures taken or proposed to be taken by Bandwidth to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects. If Bandwidth is unable to provide all of the information above as part of the initial notification, Bandwidth will provide this information to Customer as soon as reasonably practicable. Except as required by Data Protection Laws, the obligations herein will not apply to incidents that are caused by Customer. Bandwidth's notification of or response to a Security Incident will not be construed as an acknowledgement by Bandwidth of any fault or liability with respect to the Security Incident.

**6.3 Confidentiality.** Bandwidth will take reasonable steps to ensure that its personnel who have access to the Personal Data (i) are informed of the confidential nature of such information, have received appropriate training on their responsibilities, and have executed written confidentiality agreements; (ii) will protect such data in accordance with Bandwidth's confidentiality obligations under the Services Agreement and / or applicable Data Protection Laws and (iii) are obliged to keep Personal Data confidential.

## **Section 7. International Data Transfers.**

**7.1 Location of Processing.** Customer acknowledges that Bandwidth's primary processing facilities are located in the United States and Belgium, as well as in other countries outside the EEA, the UK, and Switzerland.

**7.2 EEA Restricted Transfers.** If Personal Data is transferred under this DPA from the EEA, UK, or Switzerland to countries that do not ensure an adequate level of data protection under applicable Data Protection Laws of the foregoing territories, the Parties agree to abide by and Process Personal Data as follows: (i) with regard to Personal Data for which Customer acts as a Controller, and Bandwidth as an independent Controller, in compliance with Module 1: Transfer Controller to Controller of the EU Standard Contractual Clauses ("**C2C Clauses**") and (ii) with regard to Personal Data for which Customer Acts as Controller, and Bandwidth as a Processor, in compliance with Module 2: Transfer Controller to Processor of the EU Standard Contractual Clauses ("**C2P Clauses**"), which the Parties hereby incorporate by reference into this DPA together as the "Clauses," as supplemented by the points below:

- **Data exporter and data importer.** For the sake of clarity, the Clauses apply to Customer who, for the purposes of the Clauses, acts as 'data exporter' and Bandwidth, and each of its Affiliates based outside the EEA, the UK and Switzerland, for the purposes of the Clauses, may act as 'data importer' under this DPA.
- **Docking Clause.** Clause 7 of the Clauses, the 'Docking Clause – Optional,' shall be deemed incorporated.
- **General Written Authorization.** In clause 9 of the C2P Clauses, the Parties choose Option 2 (General Written Authorization), which shall be enforced in accordance with Section 4.4 of this DPA.

- **Optional wording in Clause 11 Redress.** The optional wording in clause 11 of the Clauses shall not be deemed incorporated.
- **Governing laws.** In clause 17 of the Clauses, the Parties agree that the Clauses shall be governed by the laws of Belgium.
- **Courts.** In clause 18 of the Clauses, the Parties agree that any dispute arising from the Clauses shall be resolved by the French Courts of Tribunal Belgium.
- **Annexes.** Annex I.A, I.B and I.C of the Clauses shall be deemed completed with the information set out in Appendix 1 ( C2C) and Appendix 2 (C2P). Annex II of the Clauses shall be deemed completed with the information set out in Appendix 3.
- **Prevalence of the Clauses.** Nothing in this DPA or in the Services Agreement is intended by the Parties to be construed as prevailing over the Clauses.

**7.3 UK Restricted Transfers.** If Personal Data is transferred under this DPA from the United Kingdom to countries that do not ensure an adequate level of data protection under applicable Data Protection Laws in that territory, then the Parties (Customer as ‘data exporter’ and Bandwidth, and each of its Affiliates based outside the UK and EEA, for the purposes of the UK Addendum as ‘data importer’) further agree to the UK Addendum, which the Parties hereby incorporate by reference into this DPA and deem completed by reference to the equivalent information in Section 7.2 (EEA Restricted Transfers).

### **Section 8. Limitation of Liability.**

The total liability of each Party (and their respective employees, directors, officers, affiliates, successors, and assigns) to the other, arising out of or related to this DPA, whether in contract, tort, or other theory of liability, will not, when taken together in the aggregate, exceed the limitation of liability set forth in the Services Agreement. This section is not intended to modify or limit the parties’ joint and several liability for Data Subject claims under GDPR Article 82 or the right of contribution under GDPR Article 82. Further, this section is not intended to limit either party’s responsibility to pay penalties imposed on that party by a regulatory authority for that party’s violation of applicable Data Protection Laws.

### **Section 9. Term.**

This term of this DPA will be coextensive with the term of the Services Agreement. Each Party’s obligations under this DPA will terminate upon expiration or termination of the Services Agreement, unless otherwise mandated under applicable law, otherwise agreed by the Parties in writing, or otherwise provided in the EU Standard Contractual Clauses.

### **Section 10. Miscellaneous.**

This DPA supersedes and replaces any existing data processing addendum that the Parties may have previously entered into in connection with the Services and all prior and contemporaneous agreements, oral and written, regarding the subject matter of this DPA between Bandwidth and Customer. The Customer acknowledges and agrees that Bandwidth may update this DPA from time to time in case required as a result of (i) changes in Data Protection Laws; (ii) the release of new Services and/or features thereof or material changes thereto; (iii) a merger, acquisition, or other similar transaction; provided that Bandwidth will provide at least thirty (30) days prior written notice at the email address associated with the Customer’s account. Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Services Agreement regarding the parties’ respective privacy and security obligations, this DPA will control. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Services Agreement, except where otherwise indicated by the EU Standard Contractual clauses or Data Protection Laws.

#### **List of Appendices:**

Appendix 1 – Appendix to C2C Clauses

Appendix 2 – Appendix to C2P Clauses

Appendix 3 – Security Measures

*(The remainder of this page is intentionally left blank.)*

## Appendix 1

### Bandwidth Acting as a Controller: Details of the Processing for C2C Clauses

#### A. List of Parties

The data exporter is Customer, acting as Controller. The data importer is Bandwidth and/or its Affiliates, acting as Controller.

#### B. Description of Transfer

Categories of Data Subjects:

- Customer's commercial contacts and representatives
- Customer's Subscribers or End Users
- Calling and called parties (related to Communications Metadata)

Categories of Personal Data:

- Customer Account Information, such as name, email address, phone number
- Subscriber Data, such as name, email address, physical address, phone number and when required by law for the provision of Services and pursuant to the Services Agreement, additional categories of Personal Data such as birth date, physical address, nationality, and/or identification card of Subscriber
- Communications Metadata
- Any other category of Personal Data that the Parties may agree to collect and Process for the purpose of Bandwidth providing the Services

Sensitive Data (if applicable): N/A

Nature of the Processing:

Among others, consultation, verification, generation, storage.

Purposes of the Transfer:

The Personal Data transferred will be subject to the following Processing activities:

- Performance of electronic communications Services under the Services Agreement, which includes, but is not limited to: generation and storage of call data records, the exchange of commercial communications between Bandwidth and Customer, billing and payment, Customer administration, provisioning, verification of Customer identity and solvency, maintenance, support, fraud detection and prevention, or sales purposes;
- Compliance with applicable local laws and regulations (including but not limited to Data Protection Laws and telecommunications laws).

Frequency of the Transfer (e.g., whether the data is transferred on a one-off or continuous basis):

The transfers will be made on a continuous basis.

Period for which the Personal Data will be Processed and Retained:

For the duration of the Services Agreement and subject to Section 3.4 of this DPA.

For transfers to Subprocessors, also specify subject matter, nature, and duration of the processing:

The transfers to Subprocessor will concern the provision of the Services.

#### C. Competent Supervisory Authority

The EU country where Customer is based. If Customer is not based in the EU but is subject to the GDPR, the country of competent supervisory authority will be Belgium.

## Appendix 2

### Bandwidth Acting as a Processor: Details of the Processing for C2P Clauses

#### A. List of Parties

The data exporter is Customer, acting as Controller. The data importer is Bandwidth and/or its Affiliates, acting as Processor.

#### B. Description of Transfer

Categories of Data Subjects:

- Calling and called parties who send or receive communications via the Processor Services

Categories of Personal Data:

- Communications Content, to the extent it qualifies as Personal Data
- Any other category of personal Data that the Parties may agree to collect and Process for the purpose of Bandwidth providing the Services

Sensitive Data (if applicable):

Bandwidth does not intentionally collect or process any special categories of data in the provision of its products and/or services. However, special categories of data may from time to time be inadvertently processed by Bandwidth where the Customer or its Subscribers or end users choose to include this type of data in the communications it transmits using the Services.

Nature of the Processing:

Among others, consultation, verification, generation, storage.

Purposes of the Transfer:

The Personal Data transferred will be subject to the following Processing activities:

Bandwidth's provision of the Processor Services pursuant to the Services Agreement, including recording, storage, and analysis on behalf of Customer, as applicable; and (ii) compliance with applicable local laws (including but not limited to Data Protection Laws and telecommunications law and regulations).

Frequency of the Transfer (e.g., whether the data is transferred on a one-off or continuous basis):

Transfers will be made on a continuous basis.

Period for which the Personal Data will be Processed and Retained:

For the duration of the Services Agreement and subject to Section 4.6 of this DPA.

For transfers to Subprocessors, also specify subject matter, nature, and duration of the processing:

The transfers to Subprocessors will concern the provision of the Processor Services.

#### C. Competent Supervisory Authority

The EU country where Customer is based. If Customer is not based in the EU but is subject to the GDPR, the country of competent supervisory authority will be Belgium.

### **Appendix 3**

#### **Technical and Organizational Measures including Technical and Organizational Measures to Ensure the Security of the Data**

See [www.bandwidth.com/security](http://www.bandwidth.com/security) for information and details regarding security measures implemented by Bandwidth.

*(The remainder of this page is intentionally left blank.)*