Bandwidth Privacy Notice

Effective Date: November 18, 2024

Who we are

Hello there and welcome to our Privacy Notice! This Notice applies to Bandwidth and its affiliates (including Voxbone, which joined Bandwidth as of November 2, 2020). We are a cloud-based communications provider for enterprises. Our solutions include a broad range of software APIs for voice and text functionality, as well as our own IP voice network. A reference to **"Bandwidth," "we," "us," or "our"** is a reference to Bandwidth Inc. and its affiliates.

As used in this Privacy Notice, **"personal data"** means any information that relates to, describes, or could be used to identify an individual, directly or indirectly. This does not include anonymous or de-identified data, which does not relate to an identified or identifiable natural person or cannot be linked to or identify an individual.

This Privacy Notice applies to personal data collected by Bandwidth through the bandwidth.com website and other interactions where we provide a direct link to this Privacy Notice, including digital, paper, and in-person communications. This Privacy Notice does not cover handling of your personal data as an employee, intern, consultant, contractor or applicant of Bandwidth and does not cover any information collected by third-party sites or content or applications that may link to or be accessible from or on our websites.

Please read this Privacy Notice carefully to understand how we collect and process personal data.

Personal data that we collect

- **Identifiers,** your full name, address, email, company name, company website, telephone number, caller ID information, unique personal identifier, online identifier, Internet Protocol ("IP") address, proof of address and ID of end users (where there is a regulatory requirement).
- **Account Payment Information,** your credit/debit card number, signature, bank wire transfer information.
- **Commercial Information,** records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- **Internet or Similar Network Activity,** your browsing and search history, information on your interaction with our websites and advertisements, information about the communications delivered via our platform.

- **Metadata,** information about the communications delivered via our platform such as source and destination information, IP address, completion status, time and duration of use.
- **Geolocation Data,** when you use our products or services, such as source and destination information about the communications delivered, real-time location information for emergency service via the Bandwidth products or services.
- **Cookies and Other Technologies,** website cookies and similar technologies to distinguish you from other visitors and compile information about the usage of our websites. For further information, please see "Cookies and other tracking technologies."
- **Sensory Data,** your interactions with our sales and customer support teams may be recorded for quality assurance, training, and analysis purposes (subject to your consent if required by applicable law). When you use our products or services, it may include text-to-speech/speech-to-text transcriptions, DTMF tones, media in your voice calls and text messages.

How we collect personal data

We use different methods to collect personal data from and about you including through:

- **Direct interactions.** You may give us information about you by filling in forms, engaging in chat on our website, accessing or utilizing any of our websites, opening an account with us, requesting support, subscribing to our newsletters, requesting information or materials (e.g. whitepapers), registering for events or webinars, visiting our booth at a trade show or other event, participating in surveys or evaluations, accessing or utilizing any of our websites, submitting questions or comments, or by corresponding with us by phone, email, video, or otherwise.
- **Automated technologies or interactions.** As you interact with our websites, we may automatically collect technical data about your equipment, browsing actions, and patterns as specified above. See "Cookies and other tracking technologies."
- **Third parties or publicly available sources.** We may receive information about you if you visit other websites employing our cookies or from third parties including, for example, advertising networks, analytics providers, or through publicly available data, such as social media (like LinkedIn, Facebook, and others) and websites.
- **Indirectly.** As a service provider in the course of providing voice and messaging communications services.

How we use personal data

We may use the personal data we collect for one or more of the following purposes:

- **To fulfill or meet the reason you provided the information and to provide our products and services.**
    - To respond to your inquiry about our products and services, including to investigate and address your concerns and monitor and improve our responses.
    - To enable our customers and end users to send and receive communications via our platform and to bill for those services.
    - To inform you of additional features, expanded coverage or other products or services offered by us.
    - To allow you to interact with our systems, including our websites.
    - To create, maintain, customize and secure your account with us.
    - To process your requests, purchases, transactions and payments.
    - To bill, collect, and remit taxes, fees and surcharges to the appropriate jurisdictions.
    - To personalize your website experience and to deliver content and service information relevant to your interests, including targeted offers, marketing communications and ads through our websites, third-party sites and via email.
    - To maintain the safety, security and integrity of our website, services, databases and other technology assets and business.
    - For testing, research, development, and analysis; mitigation of fraud and spam (as applicable per specific product offering), unlawful or abusive activity, or violations of our Acceptable Use Policy; perform quality control; gauge routing effectiveness and deliverability and product development, including developing and improving our websites and products and services. Specifically, with respect to MMS and SMS messaging, we utilize industry-standard content-analysis software which utilizes electronic, algorithmic inspection of the originating telephone number and/or content of MMS and SMS messages for purposes of spam blocking (only applicable to US).
    - If you have elected to have your name, address, and telephone number published in directories, we may share such information with directory publishers (who publish white pages, yellow pages, and other similar directories) and directory assistance providers.
    - As described to you when collecting your personal data.
- **Law enforcement, security, and safety.**
    - To respond to law enforcement requests and as required by applicable law, court order, governmental regulations, or other legal process where we believe in good faith that disclosure protects your safety or the safety of others, or where we need to protect a legitimate business interest such as fighting against fraud that harms our rights.
    - For security purposes to register visitors to our offices To respond to law enforcement requests and as required by applicable law, court order, governmental regulations, or other legal process where we believe in good faith that disclosure protects your safety or the safety of others, or where we need to protect a legitimate business interest such as fighting against fraud that harms our rights.
- **Asset transfer and/or M&A Activity.**

    - To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Bandwidth's assets, whether at Bandwidth's discretion or as part of bankruptcy, liquidation, or similar proceeding, in which personal data held by Bandwidth about you is among the assets transferred.

The legal basis for collecting and using the personal data described above will depend on the personal data concerned and the specific context in which we collect it, including but not limited to: (a) performance of a contract; (b) legitimate interest; (c) necessary for compliance with a legal obligation; or (d) consent to collect and process your personal data.

Bandwidth will not use the personal data we collected for materially different, unrelated, or incompatible purposes without providing you notice. We may use non-personal data for any business purpose. To improve our products and services, we commonly will de-identify/anonymize or aggregate your personal data (so that it can no longer be associated with you), in which case we may use this information indefinitely without further notice to you.

How we share personal data

We may disclose your personal data to a third party for a business purpose, including those described in the "How we use your personal data" section above. Bandwidth may share your personal data in the following ways:

- To companies that perform services on our behalf only as needed for them to perform those services, including other communications providers in order to route communications over the Bandwidth network.
- To any member of our corporate group, which means our subsidiaries, our ultimate holding company and its subsidiaries.
- To advertising and marketing companies and networks.
- To data analytic providers.
- To other companies and entities, to:
    - Respond to emergencies or exigencies;
    - Comply with court orders, law, and other legal process, including responding to any government, public, or regulatory authority request, including to meet national security or law enforcement requirements;
    - Assist with identity verification, preventing fraud, and identity theft;
    - Provide directory assistance services, with your consent.
- To fulfill the purpose for which you provide it.
- For any other purpose that we disclose in writing when you provide the personal data.
- With your consent.
- To sell, transfer, merge, divest, restructure, reorganize, or dissolve all or a portion of our business or assets.

- To enforce our customer Services Agreement, Acceptable Use Policy, and other agreements.
- To protect the rights, property, or safety of our business, our employees, our customers, or others.

International data transfers and the EU-US Data Privacy Framework

Bandwidth is a global organization, with legal entities, business practices, and technical systems that operate across borders. Your personal data may be collected, transferred to, and stored by us in the United States and by our subsidiaries and/or third-party service providers that are in other countries. Therefore, your personal data may be transferred and processed outside your jurisdiction and in countries that may not provide for the same level of data protection as your jurisdiction, such as the European Economic Area (**"EEA"**).

Where applicable law requires us to use a data transfer mechanism, we rely on adequacy decisions as adopted by the European Commission; standard contractual clauses issued by the European Commission; or pursuant to established derogations for specific situations.

Bandwidth participates in and complies with the EU-US Data Privacy Framework (the "DPF") and the UK Extension to the DPF as set forth by the U.S. Department of Commerce. Bandwidth has certified to the U.S. Department of Commerce that it adheres to the EU-US Data Privacy Framework Principles (the "Principles") with regard to the processing of personal data received from the European Union in reliance on the DPF and from the United Kingdom (and Gibraltar if applicable) in reliance on the UK Extension to the DPF. If there is any conflict between the terms in this Privacy Notice and the Principles, the Principles will govern. To learn more about the DPF program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

In compliance with the DPF and the UK Extension to the DPF, Bandwidth commits to:

- Subject to the Principles all personal data received from the EEA in reliance on the DPF and from the United Kingdom (and Gibraltar if applicable) in reliance on the UK Extension to the DPF;
- Resolve DPF Principles-related complaints about our collection and use of your personal information. EU and United Kingdom individuals with inquiries or complaints regarding our handling of personal data received in reliance on the DPF or from the United Kingdom (and Gibraltar if applicable) in reliance on the UK Extension to the DPF should first contact our Privacy Team at privacy@bandwidth.com. For more detailed guidance please also review the information below under "Data subject rights," "Exercising your rights," and "How to contact us.";
- Cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the United Kingdom Information Commissioner's

Office (ICO) and the Gibraltar Regional Authority (GRA) (if applicable) with regard to unresolved complaints concerning our handling of personal data received in reliance on the DPF or the UK Extension to the DPF. Individuals have the possibility, under certain conditions, to invoke binding arbitration for complaints regarding DPF compliance that are not resolved by any of the other DPF mechanisms. For additional information about the arbitration process please see Annex I of the Principles: https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf?tabset-35584=2.

IIn certain circumstances, Bandwidth may transfer personal data received from the European Economic Area or from the United Kingdom (and Gibraltar if applicable) in reliance on the DPF to third parties, such as its service providers. Bandwidth maintains contracts with these parties that restrict their access, use, and disclosure of personal data and that require them to provide at least the same level of protection as required by the DPF Principles. Bandwidth is responsible for these parties' compliance with these obligations, and may be liable under the Principles if they process such personal data in a manner inconsistent with the Principles, unless Bandwidth proves that it is not responsible for the event giving rise to any damages.

Bandwidth Inc. is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC). In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

For more information regarding international data transfers among Bandwidth affiliates, please visit www.bandwidth.com/legal/data-protection-and-privacy.

Cookies and other tracking technologies

Our websites use cookies (small files placed on your device) and similar technologies (e.g., web beacons, pixels, tags, JavaScript, alone or in conjunction with cookies) to distinguish you from other visitors and compile information about the usage of our websites. These cookies and similar technologies may be provided by us or an authorized third party. This helps us deliver a better and more personalized service when you browse our websites and allows us to improve our websites. We may also use these technologies to collect information about your online activities over time and across third-party websites or other online services (known as behavioral tracking). We use both session-based and persistent cookies on our websites. Session-based cookies exist only during one session and disappear from your computer when you close your browser or turn off your computer. Persistent cookies remain on your computer or device after you close your browser or turn off your computer.

We also use web beacons on our websites and in email communications. For example, we may place web beacons in marketing emails that notify us when you click on a link in the email that

directs you to one of our websites. To unsubscribe from our marketing emails, click the link at the bottom of the email marked “Unsubscribe” or manage your Bandwidth email subscription at https://go.bandwidth.com/UnsubscribePage.html . Please note that you cannot opt out of receiving transactional emails related to our products and services.

We may disclose information to third parties or allow third parties to directly collect information using these technologies on our websites, such as social media companies, advertising networks, companies that provide analytics including ad tracking and reporting, security providers, and others that help us operate our business and websites.

The following describes how we use different categories of cookies and your options:

- **Strictly Necessary Cookies.** Strictly necessary cookies are necessary for our websites to function and cannot be switched off in our systems. Some examples include: session cookies needed to transmit the website, authentication cookies, and security cookies. If you have chosen to identify yourself to us, we may place a cookie on your device that allows us to uniquely identify you when you are logged into our websites and to process your online transactions and requests. When you visit our websites for the first time, a cookie consent banner may prompt you to customize your cookie preferences in our Cookie Preference Center. If you are in the EEA (based on IP address), our websites will only serve you strictly necessary cookies unless you consent to additional categories in our Cookie Preference Center.
- **Functional Cookies.** Functional cookies enhance function, performance, and services on our websites. They also allow us to analyze your use of our websites to evaluate and improve your customer experience on this site. For example, some of our websites use Google Analytics, a service provided by Google Inc., which uses cookies to find out how visitors use our website. To learn how Google Analytics collects and processes data, please visit: “How Google uses data when you use our partners’ sites or apps” located at www.google.com/policies/privacy/partners. If you do not allow functional cookies then some or all services may not function properly.
- **Targeting Cookies.** Targeting cookies may be set through our websites by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant advertisements on other sites. They do not store directly personal data, but are based on uniquely identifying your browser and internet device. Some examples include: cookies used for remarketing or interest-based advertising.
- **Performance Cookies.** These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our websites. They help us to know which pages are the most and least popular.

Cookie preferences

When you visit our websites for the first time, a cookie consent banner may prompt you to customize your cookie preferences. You may change your cookie settings and preferences for our websites anytime by visiting our Cookie Preference Center. You can also control the use of cookies by changing the settings in your browser. To change your web browser settings for cookies, you can follow the instructions in the help section of your web browser or visit www.allaboutcookies.org. You can also opt out of Google Analytics by downloading, installing, and enabling the Google Analytics' Opt-out Browser Add-on, which can be found at https://tools.google.com/dlpage/gaoptout/. Please note that choosing to disable cookies may limit your use of certain features or functions on our websites.

Advertising preferences

Industry third parties also provide additional tools for opting out of targeted advertising. You can access a mechanism for exercising your ad setting choices by going to https://www.aboutads.info/choices and https://www.youronlinechoices.eu/. Please note these opt-out tools are provided by third parties and are not controlled by us.

Do not track

Do not track is a privacy preference that you can set in your web browser. When you turn on the do not track signal, the browser sends a message to websites requesting them not to track you. For information about do not track, visit http://www.allaboutdnt.org. At this time, we do not respond to do not track browser settings or signals.

Global Privacy Control

Global privacy control is a browser-based technical specification that you can use to signal your privacy preference for behavioral advertising. Certain browsers and extensions will allow you to enable GPC or enable GPC by default; you can learn more at globalprivacycontrol.org. If you enable GPC, our cookie preferences tool will automatically turn off all targeting cookies on our websites in response to the signal from that browser or device.

Data subject rights

You have certain rights regarding our processing of your personal data under applicable data protection laws. This section describes these rights and how you can exercise them. Please

note these laws may provide limitations or exceptions that apply to these rights. We have described these rights generally, without noting all applicable jurisdictions, limitations, or exceptions. When you make a request to exercise any of these rights, we may provide more detailed information regarding any exceptions or limitations that apply.

- **Right to know.** You have the right to ask us to confirm whether or not we process your personal data, the categories of personal data we have collected and the sources from which we collect it, our purposes for collecting your personal data, the categories of third parties to whom we disclose your personal data, and the specific pieces of personal data we have collected about you.
- **Right to access.** You have the right to request a copy of your personal data and supplementary information.
- **Right to correction/rectification.** You have the right to request that we correct any information you believe is inaccurate. You also have the right to request that we complete information you believe is incomplete.
- **Right to erasure/deletion.** You have the right to request that we erase or delete your personal data, under certain circumstances and subject to certain exceptions.
- **Right to restriction of processing.** You have the right to restrict the processing of your personal data, under certain circumstances, including, depending on applicable law and the jurisdiction in which you reside or are located, opting out of disclosures of personal information to an unaffiliated third party who does not serve as our agent or service provider, if any, or (b) use of personal information for a purpose other than the purpose for which it was originally collected or subsequently authorized if any such use occurs.
- **Right to data portability.** You have the right to receive personal data you have provided to us in a structured, commonly used and machine-readable format that allows you to transmit the data to another controller without hindrance. You also have the right to request that we transmit this data directly to another controller.
- **Right to withdrawal of consent.** In the event our processing of your personal data is based on your consent, you may withdraw your consent at any time. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.
- **Right to object to processing.** You have the right to object to the processing of your personal data at any time, under certain circumstances.
- **Right to opt out of our processing, "sale," or sharing of personal data for targeted or cross-context behavioral advertising**. You have the right to opt out of our processing, "sale" (as that term is broadly defined in the California Consumer Privacy Act), or sharing of your personal data for targeted or cross-context behavioral advertising, which means displaying advertising to you based on personal data obtained or inferred from your activities over time across different websites, applications, and other online services we do not operate. As detailed in the Cookies section above, you may exercise this right by visiting our Cookie Preference Center to disable targeting cookies. You may also opt out of the processing or sharing of your personal data for targeted or cross-context behavioral advertising in a frictionless manner through the use of an opt-out preference signal such as Global Privacy Control. Please see the Cookies section above for additional details on how to implement these settings and other

advertising preferences. Please note that even if you opt out of allowing us to use or disclose your personal data for targeted or cross-context behavioral advertising, you may still see our ads on other websites, applications, and online services, and we may still base aspects of our advertising on your interactions with us and our websites.

- **Non-Retaliation.** You have a right not to receive discriminatory treatment for exercising the rights described above.

Exercising your rights

Except as otherwise noted above, to exercise any of the above rights or if you have any questions about this Privacy Notice, please submit them through our DATA SUBJECT RIGHT REQUEST FORM. US residents may also call us toll-free at 866-824-2792.

- **Making a Request; requests by others on your behalf.** Only you, or someone legally authorized to act on your behalf (this includes an authorized agent), may make a verifiable consumer request related to your personal data using the methods described above. The response we provide will also explain the reason we cannot comply with a request, if applicable.
- **Fees.** You will not have to pay a fee to access your personal data or to exercise any of the other rights. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.
- **Information we may need from you.** We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data or to exercise any of your other rights, such as your first and last name, email address, mailing address, telephone number, or other information necessary to verify your identity or that your representative is authorized to act on your behalf. This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to assist with our response. Any personal data provided to us for verification and fraud-prevention purposes will only be used for that purpose and such information will be deleted as soon as practical after processing your consumer request.
- **Timing.** We try to respond to all legitimate requests within one month of receipt of the request. Occasionally, it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.
- **Appeals.** If we refuse to take action on your request, you may appeal that refusal by contacting us through our DATA SUBJECT RIGHT REQUEST FORM or calling us toll-free at 866-824-2792.

You may also make a complaint about our processing of your personal data to a relevant data protection supervisory authority. We would, however, appreciate the opportunity to address your concerns before you do so.

How long we retain your personal data

We will only retain your personal data for as long as reasonably necessary to fulfill the purposes we collected it for, including the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means and the applicable legal, regulatory, tax, accounting or other requirements. After expiration of the applicable retention periods, your personal data will be deleted or anonymized. If there is any personal data that we are unable, for technical reasons, to delete entirely from our systems, we will put in place appropriate measures to prevent any further use of such personal data. To improve our products and services, we commonly will aggregate your personal data (so that it can no longer be associated with you), in which case we may use this information indefinitely without further notice to you.

How we protect your personal data

Bandwidth takes precautions including administrative, technical, and physical measures to help safeguard against the accidental or unlawful destruction, loss, alteration and unauthorized disclosure of, or access to, the personal data we process or use. Please note, though, that no provider can guarantee security, especially when providing services that rely on the public internet or during transmission through the interconnected landscape of telecommunications. You are solely responsible for protecting your account password(s), limiting access to your devices, and signing out of websites after your sessions. You are responsible for any activity conducted using your credentials or passwords. If you believe your password to any of our websites or systems have been compromised, please notify us immediately at privacy@bandwidth.com.

Linked websites

For your convenience, hyperlinks may be posted on our websites that link to other websites (**“third-party sites”**). We are not responsible for the privacy practices of any third-party sites or of any companies that we do not own or control. This Privacy Notice does not apply to third-party sites. Third-party sites may collect information in addition to that which we collect on our websites. We do not endorse any of these third-party sites, the services or products described or offered on such third-party sites, or any of the content contained on the

third-party sites. We encourage you to read the privacy notice of each third-party site that you visit to understand how the information that is collected about you is used and protected.

Children

Our websites, products, and services are not directed to children (under the age of 13 in the United States or under the age of 16 in the EEA) and we do not knowingly collect online personal data directly from children. If you are a parent or guardian of a minor child and believe that the child has disclosed online personal data to us, please contact us at privacy@bandwidth.com.

Changes to this Privacy Notice

We may update this Privacy Notice from time to time. When we do so, we will post the updated Privacy Notice on our website and update the Privacy Notice's Effective Date. We will notify you of material changes to this Privacy Notice by placing a prominent notice at the top of the Privacy Notice and/or by sending a notice to the customer email address you have provided us.

How to contact us

If you have questions about this Privacy Notice, please contact the Bandwidth Privacy Team at privacy@bandwidth.com.

To contact us in writing, please use:

Bandwidth Inc.
Attn: Legal – Privacy
2230 Bandmate Way
Raleigh, NC 27607 USA