Bigtincan Privacy Policy

This Privacy Policy provides our policies and procedures for collecting, using, and disclosing your information. Users can access the Bigtincan Hub service (the "**Service**") through our website www.Bigtincan.com, applications on Devices, through APIs, and through third-parties. A "**Device**" is any computer used to access the Bigtincan Service, including without limitation a desktop, laptop, mobile phone, tablet, or other consumer electronic device. This Privacy Policy governs your access of all products and services provided by Bigtincan, regardless of how you access them, and by using our Services you consent to the collection, transfer, processing, storage, disclosure and other uses described in this Privacy Policy. All of the different forms of data, content, and information described below are collectively referred to as "information." As indicated by the attached documentation, additional policies apply to Bigtincan's VoiceVibes and Brainshark products.

1. The Information We Collect And Store

We may collect and store the following information when running the Bigtincan Service:

Information You Provide. When you register an account, we collect some personal information, such as your name, phone number, credit card or other billing information, email address and home and business postal addresses. You may also ask us to import your contacts by giving us access to your third-party services (for example, your email account) or to use your social networking information if you give us access to your account on social network connection services. You may also provide us with your contacts' email addresses when sharing folders or files with them. We may also receive Personal Information (for example, your email address) through other users, for example, if they have tried to share something with you.

Files. We collect and store the files you upload, download, or access with the Bigtincan Service ("**Files**"). If you add a file to your Bigtincan Hub that has been previously uploaded by you or another user, we may associate all or a portion of the previous file with your account rather than storing a duplicate.

Log Data. When you use the Service, we automatically record information from your Device, its software, and your activity using the Services. This may include the Device's Internet Protocol ("IP") address, browser type, the web page visited before you came to our website, information you search for on our website, locale preferences, identification numbers associated with your Devices, your mobile carrier, date and time stamps associated with transactions, system configuration information, metadata concerning your Files, and other interactions with the Service.

2. How We Use Personal Information

Personal Information. In the course of using the Service, we may collect personal information that can be used to contact or identify you ("**Personal Information**"). Personal Information is or may be used: (i) to provide and improve our Service, (ii) to administer your use of the Service, (iii) to better understand your needs and interests, (iv) to personalize and improve your experience, and (v) to provide or offer software updates and product announcements. If you no longer wish to receive communications from us, please follow the "unsubscribe" instructions provided in any of those communications, or update your account settings information.

Geo-Location Information. Some Devices allow applications to access real-time location-based information (for example, GPS). Our mobile apps do not collect such information from your mobile device at any time while you download or use our mobile apps as of the date this policy went into effect but may do so in the future with your consent to improve our Services. Some photos and videos you place in Bigtincan Hub may contain recorded location information. We may use this information to optimize your experience. If you do not wish to share files embedded with your geo-location information with us, please do not upload them. If you don't want to store location data in your photos or videos, please consult the documentation for your camera to turn off that feature. Also, some of the information we collect from a Device, for example IP address, can sometimes be used to approximate a Device's location.

Analytics. We also collect some information (ourselves or using third party services) using logging, such as IP address, which can sometimes be correlated with Personal Information. We use this information for the above purposes and to monitor and analyze use of the Service, for the Service's technical administration, to increase our Service's functionality and user-friendliness, and to verify users have the authorization needed for the Service to process their requests.

3. Information Sharing and Disclosure

Your Use. Any information you choose to provide should reflect how much you want others to know about you. Please consider carefully what information you disclose and your desired level of anonymity. We do not sell your personal information to third parties. We may also share or disclose your information with your consent, for example, if you use a third-party application to access your account (see below). Through certain features of the Service, you may also have the ability to make some of your information public. Public information may be broadly and quickly disseminated.

Service Providers, Business Partners and Others. We may use certain trusted third-party companies and individuals to help us provide, analyze, and improve the Service (including but not limited to data storage, maintenance services, database management, web analytics, payment processing, and improvement of the Service's features). These third parties may have access to your information only for purposes of performing these tasks on our behalf and under obligations similar to those in this Privacy Policy.

Third-Party Applications. We may share your information with a third party application with your consent, for example when you choose to access our Services through such an application. We are not responsible for what those parties do with your information, so you should make sure you trust the application and that it has a privacy policy acceptable to you.

Compliance with Laws and Law Enforcement Requests; Protection of Bigtincan's Rights. We may disclose to parties outside Bigtincan Hub files stored in your Bigtincan Hub and information about you that we collect when we have a good faith belief that disclosure is reasonably necessary to (a) comply with a law, regulation or compulsory legal request; (b) protect the safety of any person from death or serious bodily injury; (c) prevent fraud or abuse of Bigtincan Hub or its users; or (d) to protect Bigtincan's property rights. If we provide your Bigtincan Hub files to a law enforcement agency as set forth above, we will remove Bigtincan's encryption from the files before providing them to law enforcement. However, Bigtincan will not be able to decrypt any files that you encrypted prior to storing them on Bigtincan Hub.

Business Transfers. If we are involved in a merger, acquisition, or sale of all or a portion of our assets, your information may be transferred as part of that transaction, but we will notify you (for example, via email and/or a prominent notice on our website) of any change in control or use of your Personal Information or Files, or if either become subject to a different Privacy Policy. We will also notify you of choices you may have regarding the information.

Non-private or Non-Personal Information. We may disclose your non-private, aggregated, or otherwise non-personal information, such as usage statistics of our Service.

4. Changing or Deleting Your Information

If you are a registered user, you may review, update, correct or delete the Personal Information provided in your registration or account profile by changing your "account settings." If your personally identifiable information changes, or if you no longer desire our service, you may update or delete it by making the change on your account settings. In some cases we may retain copies of your information if required by law. For questions about your Personal Information on our Service, please contact info@Bigtincan.com. We will respond to your inquiry within 30 days.

5. Data Retention

We will retain your information for as long as your account is active or as needed to provide you services. If you wish to cancel your account or request that we no longer use your information to provide you services, you may delete your account by contacting us at info@Bigtincan.com. We may retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. Consistent with these requirements, we will try to delete your information quickly upon request. Please note, however, that there might be latency in deleting information from our servers and backed-up versions might exist after deletion. In addition, we do not delete from our servers files that you have in common with other users.

6. Bigtincan Community

Our Service offers publicly accessible community services such as blogs, forums, and wikis. You should be aware that any information you provide in these areas may be read, collected, and used by others who access them. Your posts may remain even after you cancel your account. For questions about your Personal Information on our Service, please contact security@bigtincan.com.

Our Site includes links to other Web sites whose privacy practices may differ from those of Bigtincan. If you submit personal information to any of those sites, your information is governed by their privacy statements. We encourage you to carefully read the privacy statement of any Web site you visit.

7. Security

The security of your information is important to us. When you enter sensitive information (such as a credit card number) on our order forms, we encrypt the transmission of that information using secure socket layer technology (SSL).

We follow generally accepted standards to protect the information submitted to us, both during transmission and once we receive it. No method of electronic transmission or storage is 100% secure, however. Therefore, we cannot guarantee its absolute security. If you have any questions about security, you can contact us at security@bigtincan.com.

8. Our Policy Toward Children

Our Services are not directed to persons under 16. We do not knowingly collect personally identifiable information from children under 16. If a parent or guardian becomes aware that his or her child has provided us with Personal Information without their consent, he or she should contact us at info@Bigtincan.com. If we become aware that a child under 16 has provided us with Personal Information, we will take steps to delete such information from our files.

9. GDPR

While Bigtincan applies the same level of care to its customers around the world, Bigtincan also complies with the European Union's General Data Protection Regulation ("GDPR"), which went into effect on May 25, 2018. Specifically, Bigtincan complies with the GDPR requirements by providing its customers with full knowledge

of what data is transferred from a customer environment and how Bigtincan encrypts the data, whether it is in transit or at rest, ensuring in accordance with the GDPR that the data would be unintelligible to any person who is not authorized to access it. As a data processor of data provided by our customers, you can learn more about how Bigtincan treats data and complies with the GDPR by reviewing our Data Processing Addendum which is available upon request from Bigtincan. We offer our customers a Data Processing Addendum (DPA), which incorporates the EU Standard Contractual Clauses ("SCCs," also known as the EU Model Clauses) and include Bigtincan's organizational measures. The SCCs are a valid and recognized legal mechanism for ensuring that any personal data leaving the European Economic Area will be transferred in compliance with EU data-protection laws. Bigtincan continues to maintain the operational processes necessary to meet the stringent SCC requirements for the transfer of personal data to processors, which in turn allows us to provide our customers with contractual guarantees for the protection of their personal data. Bigtincan offers a DPA that includes GDPR-specific language to ensure that Bigtincan and our customers have appropriate GDPR-specific contractual provisions in place to allow for the legal transfer of personal data.

If you have questions regarding either of these statements or to obtain additional documentation, you may view our website or contact us at gdpr@Bigtincan.com.

10. Contacting Us

If you have any questions about this Privacy Policy, please contact us at: Level 6, 338 Pitt Street, New South Wales Australia 2000, or security@bigtincan.com.

11. Changes to our Privacy Policy

This Privacy Policy may change from time to time. If we make a change to this privacy policy that we believe materially reduces your rights, we will provide you with notice (for example, by email). And we may provide notice of changes in other circumstances as well. By continuing to use the Service after those changes become effective, you agree to be bound by the revised Privacy Policy.

Privacy Notice for California Residents

Effective Date: January 1, 2020

Last Reviewed on: February 15, 2020

This Privacy Notice for California Residents supplements the information contained in Bigtincan's Privacy policy and applies solely to all visitors, users, and others who reside in the State of California ("consumers" or "you"). We adopt this notice to comply with the California Consumer Privacy Act of 2018 (CCPA) and any terms defined in the CCPA have the same meaning when used in this notice.

Information We Collect

Our Website collects information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device ("personal information"). In particular, Bigtincan's website, https://www.bigtincan.com/ ("Website"), has collected the following categories of personal information from its consumers in California within the last twelve (12) months:

Category	**Examples**	**Collected**

A. Identifiers.	Name, email address, telephone number, Internet Protocol address.	YES
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	Name, email address, telephone number. Some personal information included in this category may overlap with other categories.	YES
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	NO
D. Commercial information.	Records of Bigtincan products or services considered on our website.	YES
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	NO
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	YES
G. Geolocation data.	Physical location or movements.	YES
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	NO
I. Professional or employment-related information.	Current or past job history or performance evaluations.	NO
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	NO

K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	NO

Personal information does not include:

- Publicly available information from government records.
- Deidentified or aggregated consumer information.
- Information excluded from the CCPA's scope, like:
- Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data;
- Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

Bigtincan obtains the categories of personal information listed above from the following categories of sources:

- Directly from you. For example, from forms you complete.
- Indirectly from you. For example, from observing your actions on our Website.

Use of Personal Information

We may use, or disclose the personal information we collect for one or more of the following business purposes:

- To fulfill or meet the reason you provided the information. For example, if you share your name and contact information or ask a question about our products or services, we will use that personal information to respond to your inquiry.
- To provide, support, personalize, and develop our Website, products, and services.
- To process your information requests.
- To provide you with support and to respond to your inquiries, including to investigate and address your concerns and monitor and improve our responses.
- To personalize your Website experience and to deliver content and product and service offerings relevant to your interests, including targeted offers and ads through our Website, third-party sites, and via email or text message (with your consent, where required by law).
- To help maintain the safety, security, and integrity of our Website, products and services, databases and other technology assets, and business.
- For testing, research, analysis, and product development, including to develop and improve our Website, products, and services.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your personal information or as otherwise set forth in the CCPA.

Bigtincan will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sharing Personal Information

Bigtincan may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract.

We share your personal information with the following categories of third parties:

- Service providers.
- Data aggregators.

Disclosures of Personal Information for a Business Purpose

In the preceding twelve (12) months, Company has disclosed the following categories of personal information for a business purpose:

[Category A: Identifiers.]

[Category B: California Customer Records personal information categories.]

[Category D: Commercial information.]

[Category F: Internet or other similar network activity.]

[Category G: Geolocation data.]

We disclose your personal information for a business purpose to the following categories of third parties:

- Service providers.
- Data aggregators

Sales of Personal Information

In the preceding twelve (12) months, Company has not sold personal information

Your Rights and Choices

The CCPA provides consumers (California residents) with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights.

Access to Specific Information and Data Portability Rights

You have the right to request that Bigtincan disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request (see *Exercising Access, Data Portability, and Deletion Rights*), we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting that personal information.
- The categories of third parties with whom we share that personal information.

- The specific pieces of personal information we collected about you (also called a data portability request).
- If we disclosed your personal information for a business purpose, providing disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.

Deletion Request Rights

You have the right to request that Bigtincan delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request (see *Exercising Access, Data Portability, and Deletion Rights*), we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

1. Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
4. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
5. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 *et. seq.*).
6. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
7. Comply with a legal, regulatory or other governmental obligation.
8. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

Exercising Access, Data Portability, and Deletion Rights

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by either:

- Phone: (617) 981-7557
- Email: security@bigtincan.com
- Physical Address: Bigtincan Mobile Pty Ltd, Level 6, 338 Pitt Street, Sydney, New South Wales, Australia 2000.

Only you, or a person registered with the California Secretary of State that you authorize to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.

- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you.

Making a verifiable consumer request does not require you to create an account with us. However, we do consider requests made through your password-protected account sufficiently verified when the request relates to personal information associated with that specific account.

We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Response Timing and Format

We endeavor to respond to a verifiable consumer request within thirty (30) days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing.

If you have an account with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option.

Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

Other California Privacy Rights

California's "Shine the Light" law (Civil Code Section § 1798.83) permits users of our Website that are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please send an email to privacy@bigtincan.com or write us at:

Attn: Bigtincan Privacy officer

Phone: (617) 981-7557

Email: security@bigtincan.com

Address: Bigtincan Mobile Pty Ltd, Level 6, 338 Pitt Street, Sydney, New South Wales, Australia 2000

Changes to Our Privacy Notice

Bigtincan reserves the right to amend this privacy notice at our discretion and at any time. When we make changes to this privacy notice, we will post the updated notice on the Website and update the notice's effective date. Your continued use of our Website following the posting of changes constitutes your acceptance of such changes.

Contact Information

If you have any questions or comments about this notice, the ways in which Bigtincan collects and uses your information described below and in the Privacy policy, your choices and rights regarding such use, or wish to exercise your rights under California law, please do not hesitate to contact us at:

Phone: (617) 981-7557

Website: https://www.bigtincan.com/

Email: security@bigtincan.com

Postal Address:

Bigtincan Mobile Pty Ltd

Attn: Legal – Global Privacy Officer

Level 6, 338 Pitt Street, Sydney, New South Wales, Australia 2000

Brainshark, Inc. Privacy Policy

Brainshark, Inc. a wholly owned subsidiary of Bigtincan ("Brainshark, "we," or "us") is committed to protecting the privacy of your information and wants you to be familiar with how we collect, use, and disclose information. This Privacy Policy describes our information and privacy practices with regard to our websites and applications.

1. Websites Covered

This Privacy Policy covers the information and privacy practices of Brainshark on all of its websites, including but not limited to https://www.brainshark.com (https://www.brainshark.com), and all of its applications. including but not limited to mobile applications (collectively referred to as "Brainshark's Websites" or "Websites"). The use of information collected through Brainshark's services will be limited to the purpose of providing and enhancing the service for which the Customer has engaged Brainshark.

Brainshark's Websites may contain links to third party sites that are not owned or controlled by Brainshark. Additionally, Brainshark's services are used by customers to deliver video presentations that are embedded and linked within their own websites and third-party sites. Brainshark is not responsible for the information practices or content of its customers or third-party sites. Please be aware that we are not responsible for the privacy practices of such other sites. We encourage you to be aware when you leave Brainshark's Websites and to read the privacy policies of each and every website that collects personally identifiable information. This Privacy Policy applies only to information collected by Brainshark's Websites.

2. Information Collected

Brainshark offers a variety of applications and services that are collectively referred to as the "Services." Brainshark collects information from individuals who visit Brainshark's Websites ("Visitors") and individuals who register to use the Services ("Customers"). Customers include both paying subscribers as well as subscribers of its free services. Customers should refer to www.brainshark.com (http://www.brainshark.com) and Brainshark's Terms and Conditions (//www.brainshark.com/company/terms-conditions) for the appropriate offering.

The types of information Brainshark collects may include:

- Information you provide to Brainshark - When expressing an interest in obtaining additional information about the Services or registering to use the Services, Brainshark may require you to provide personal contact information such as your name, your company name, your job title or role, your address, your phone number, and your email address.

- Website navigational information - Brainshark uses commonly used information-gathering tools, such as cookies and Web beacons, to collect information as you navigate Brainshark's Websites ("Website Navigational Information"). This Website Navigational Information includes standard information from your web browser (such as browser type, version, and language), your Internet Protocol ("IP") address, and the actions you take on Brainshark's Websites (such as, pages viewed, links clicked).

- Information you publish to Brainshark blogs or public portals - Brainshark's Websites include public blogs and portals that allow Visitors to submit and publish comments.

- Billing information - Where Brainshark permits purchases to be made directly through its Websites, Brainshark may require you to provide billing information, such as your billing name, address, and email address.

- Information you provide to Customers - A capability of the Services allows Customers to request registration information from viewers of their video presentation content. For example, presentations created by our Customers may include a guest book registration form. Brainshark is not responsible for the information practices of its Customers, and does not access this information except with a Customer's permission to provide support and assistance.

3. Use of Information Collected

Brainshark uses data about Visitors and Customers to perform the following actions:

- To respond to your request - such as to create a Brainshark account, provide login information for a webinar for which you have registered, or provide technical support.

- For marketing purposes - Brainshark may use information that Visitors provide to contact them to further discuss their interest in the Services and to send them information regarding Brainshark or its Services.

- To improve Brainshark's Websites and products - Brainshark may use Website Navigational Information to provide Visitors and Customers with relevant content and in the aggregate to identify trends and usage patterns.

- To deliver messages that help you use the Service – As part of helping its Customers use the Service effectively, Brainshark communicates with its Customers about new features and product releases, best practices, scheduled site maintenance notifications, customer events, and more. To increase the relevancy of this information, communications may be customized to your designated user role within an application (for example: administrator, author), the products or editions you have specifically licensed, or your usage of the application.

- To process your payment - Brainshark uses billing information solely to process payment for Services for which the Customer has provided that information. Brainshark utilizes a third-party payment service to process credit card payments. Credit card information is sent directly by you to the third-party payment service. Brainshark does not have access to your full credit card number and does not store such information in its own systems. Brainshark is not responsible for the third-party payment service's information practices or compliance with any applicable laws.

- To deliver the features of the Service – Customers use the Services to create, share, and track online and mobile video presentations. As part of the sharing feature, Customers

may provide the email address of an individual with whom they wish to share presentations via the Services. Brainshark uses this information only to provide the share function of the Services. Tracking information includes the date and time that a presentation was viewed, IP address and location, what portions of the presentation were viewed and in what order, and responses to interactive questions or surveys. Individuals may be associated with this tracking information, either through information they provide to the Customer, or by a unique identifier that the Customer has associated with an individual and has passed to a personalized presentation URL. Reporting and notification features enable Customers to receive tracking information via emailed reports or to pass data to their other systems. Brainshark does not use or access information about individuals that is collected by its Customers in their use of the Services except with such Customers' permission in providing support and assistance. Brainshark does not sell this information.

4. Sharing of Information Collected

We will share your personal information with third parties only in the ways that are described in this Privacy Policy.

Unless described in this Privacy Policy, Brainshark does not share, sell, rent, or trade any information collected through its Websites or Services with third parties for their promotional purposes.

Brainshark occasionally partners with third parties who co-sponsor events with Brainshark (such as webinars and other live events). In these cases, both parties may share personal information that you provide when registering for the co-sponsored event to allow the co-sponsor to contact you regarding products, programs, services, and promotions that they believe may be of interest to you. While Brainshark chooses to partner with reputable third parties that respect your information, Brainshark is not responsible for the information practices of its third-party partners.

In certain situations, Brainshark may be required to disclose information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

We reserve the right to disclose your information as required by law and when we believe that disclosure is necessary to protect our rights or to comply with a judicial proceeding, court order, or legal process.

In the event that Brainshark is a party to a merger with, or acquisition by, another company, or its assets are otherwise entirely or substantially acquired, your information will be among the assets transferred. You will be notified via email or prominent notice on our Websites, for thirty (30) days or the timeframe as defined and required by statute or regulation, of any such change in ownership or control of your personal information. Information concerning deletion or removal of your personal information or any changes that you wish to make to your personal information will be made available at that time.

5. Communications Preferences

Brainshark partners with third parties to either display advertising on our website or to manage our advertising on other sites. Our third-party partners may use technologies such as cookies to gather information about your activities on this site and other sites in order to provide you advertising based upon your browsing activities and interests. If you wish to not have this information used for the purpose of serving you interest-based ads, you may elect to turn off cookies or use your browser's privacy settings to mask your identity, or you may opt-out by the following consumer choice mechanisms, please visit:

Digital Advertising Alliance (DAA)'s self-regulatory opt-out page (http://optout.aboutads.info/ (http://optout.aboutads.info/)) and mobile application-based "AppChoices" download page (https://youradchoices.com/appchoices (https://youradchoices.com/appchoices))

-European Interactive Digital Advertising Alliance (EDAA)'s consumer opt-out page (http://youronlinechoices.eu (http://youronlinechoices.eu/))

-Network Advertising Initiative (NAI)'s self-regulatory opt-out page (http://optout.networkadvertising.org/ (http://optout.networkadvertising.org/)).

Please note you will continue to receive generic ads.

Brainshark offers Customers and Visitors who provide contact information a means to choose how Brainshark uses the information provided. Visitors and any recipients of marketing messages from Brainshark may click on the “unsubscribe” link located on the bottom of the Brainshark’s marketing emails. Customers can change their communication preferences at any time through their profile page when logged in to the Service or you can decide not to receive communications that help you use the Service.

Some email communications are part of the Services, such as the ability to receive reports or view notifications via email. For help in managing these emails, contact support@brainshark.com (mailto:support@brainshark.com).

Customers do not have the option to cancel receiving transactional emails related to their account with Brainshark or the Services.

For certain editions of the Services, Brainshark may need to communicate with the primary business contact or site administrators of a Customer's company.

6. Public Blogs, Portals, and Customer Articles

Brainshark's Websites include public blogs, portals, and customer articles that allow Visitors to submit and post comments. Brainshark also provides portal solutions for its customers.

Any personal information you choose to submit in these forums may be read, collected, or used by others who visit these forums. Brainshark is not responsible for the personal information you choose to submit to public forums for posting. If you do not want information to be public, please do not post it to these forums. To request removal of your personal information from our blog, portals, or customer articles contact us at support@brainshark.com (mailto:support@brainshark.com). In some cases, Brainshark may not be able to remove your personal information, but we will notify you via email if we are unable to do so and briefly explain the reasons.

Our blog is also managed by a third-party application that may require you to register to post a comment. We do not have access or control of the information posted to the blog managed by that third-party application. You will need to contact or login into the third-party application if you want the personal information that was posted to the comments section removed. To learn how the third-party application uses your information, please review their privacy policy.

7. Transfer of Information

Your information may be transferred to and maintained on information systems located outside of your state, province, or other governmental jurisdiction where the privacy laws may not be as protective as those in your jurisdiction. If you are located outside of the United States and choose to provide personal information to us, Brainshark transfers the information to the United States and processes it there. Regarding these data flows, Brainshark participates in the EU-U.S. and the Swiss-U.S. Privacy Shield Frameworks ("Privacy Shield"), and is

committed to applying the Privacy Shield Principles to all personal information received from countries in the European Economic Area (EEA) and Switzerland in reliance on the Privacy Shield.

8. EU-U.S. and Swiss-US Privacy Shield

Brainshark complies with the *EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Frameworks* (Privacy Shield) as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the *European Union and the United Kingdom and Switzerland,* to the United States in reliance on Privacy Shield. *Brainshark* has certified to the Department of Commerce that it adheres to the Privacy Shield Principles with respect to such information. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/ (https://www.privacyshield.gov/).

Brainshark is responsible for the processing of personal data it receives, under each Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. Brainshark complies with the Privacy Shield Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, Brainshark is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. 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.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request (https://feedback-form.truste.com/watchdog/request).

Under certain conditions, more fully described on the Privacy Shield website [https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint], you may invoke binding arbitration when other dispute resolution procedures have been exhausted.

9. Passive Collection

As is true of most websites, we gather certain information automatically. This information may include Internet protocol (IP) addresses, browser type, Internet service provider (ISP), referring/exit pages, the files viewed on our site (e.g., HTML pages, graphics, etc.), operating system, date/time stamp, and/or clickstream data to analyze trends in the aggregate and administer the site.

10. Tracking Technologies

Brainshark and its partners use cookies or similar technologies to analyze trends, administer the website, track users' movements around the website, and to gather demographic information about our user base as a whole. You can control the use of cookies at the individual browser level, but if you choose to disable cookies, it may limit your use of certain features or functions on our Websites or Services.

11. Childrens' Privacy

Brainshark's Websites and the Services are not directed to individuals under the age of 18. As Brainshark provides Services to businesses and business professionals, Brainshark does not knowingly contact or collect personal information from children under the age of 16. If an adult becomes aware that a child in their care has provided Brainshark with personal information, they should contact us at support@brainshark.com (mailto:support@brainshark.com). If you believe that we have mistakenly or unintentionally collected such information, please notify us at the contact address below so that we may immediately delete the information from our servers.

12. Security

To prevent unauthorized access or disclosure, to maintain data accuracy, to allow only the appropriate exercise of Customers' personal information while also protecting the confidentiality, integrity, and availability of Customers' personal information, Brainshark employs a variety of industry standard security technologies. Security is provided on the data, application, and hosting level. The security infrastructure includes a physically secure data center, proven firewall protection, intrusion prevention measures, role-based authorization, and additional proprietary security measures. Additional security of Customer login and presentation content is provided as part of Brainshark's Services. Please refer to the products section of www.brainshark.com (http://www.brainshark.com) or contact Brainshark's sales team for more information about included features and options that can be configured specifically for Customers' needs. These options vary by the product licensed.

Brainshark limits access to Customers' personal information and data to those Brainshark and third-party persons who have a specific business purpose for maintaining and processing such information. Brainshark employees and third-party persons who have access to Customers' personal information are made aware of their responsibilities to protect the confidentiality, integrity, and availability of that information and have been provided training or instructions on how to do so.

When you enter personal or sensitive information on Brainshark's order forms, Brainshark will encrypt the transmission of that information using reasonable security.

If you have any questions about security on our Websites, you can contact us at support@brainshark.com (mailto:support@brainshark.com).

13. Data Subjects' Rights

Upon request, Brainshark will provide you with information about whether we hold, or process on behalf of a third party, any of your personal information. To request this information please contact us at support@brainshark.com (mailto:support@brainshark.com).

You may access, correct, or request deletion of your personal information by logging in to your account, contacting us at support@brainshark.com (mailto:support@brainshark.com) or by completing this form (//www.brainshark.com/contact-sales).

Brainshark collects information under the direction of its Customers and has no direct relationship with the individuals whose personal information it processes. If you are an individual who would no longer like to be contacted by one of our Customers through the use of our Services, please contact the Customer that you interact with directly. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data should direct their query to the applicable Customer (the data controller). If requested to remove data, we will respond within a reasonable timeframe.

We may transfer personal information to companies that help us provide our Services. Transfers to subsequent third parties are covered by the service agreements with our Customers.

In certain circumstances we may be required by law to retain your personal information including personal information we process on behalf of our Customers or may need to retain your personal information in order to continue providing a Service.

14. Right to lodge a complaint

If you believe that Brainshark is not processing your personal information in accordance with the requirements set out herein or applicable EEA data protection laws, you can at any time lodge a complaint with the data protection authority of the EEA country in which you live.

For more information on how to contact the EU Data Protection Authorities, click here (http://ec.europa.eu/newsroom/article29/news-overview.cfm).

For more information on how to contact the Swiss Federal Data Protection and Information Commissioner, click here (https://www.edoeb.admin.ch/edoeb/en/home.html).

15. Additional Important Information

Sharing with Service Providers

We may share your information with third parties who provide services on our behalf to help with our business activities. These companies are authorized to use your personal information only as necessary to provide these services to us.

These services may include:

- Payment processing
- Providing customer service
- Sending marketing communications

Brainshark reserves the right to use or disclose information provided if required by judicial inquiry, court order, law, or regulation and/or Terms and Conditions or if Brainshark reasonably believes that use or disclosure is necessary to protect Brainshark's rights.

16. Social Media Widgets

Brainshark's Websites may include social media features, such as the Facebook "Like" button, and widgets, such as the "Share This" button or interactive mini-programs that run on our Websites. These features may collect your Internet protocol address, which page you are visiting on our Websites, and may set a cookie to enable the feature to function properly. Social media features and widgets are either hosted by a third party or hosted directly on our Websites. Your interactions with these features or widgets are governed by the privacy statement of the company providing them.

17. Updates to this Privacy Policy

We may update this Privacy Policy periodically to reflect changes to our information and privacy practices. If we make any material changes, we will notify you by email (sent to the e- mail address specified in your account) or by means of a written notice on our Websites prior to the change becoming effective. We encourage you to periodically review this page for the latest information about Brainshark's information and privacy practices.

18. Contacting Us

Contact info@brainshark.com (mailto:info@brainshark.com) for questions regarding this Privacy Policy or the information and privacy practices of Brainshark's Websites.

If you are a Customer and would like help managing your communication preferences, please contact support@brainshark.com (mailto:support@brainshark.com).

Brainshark's data protection officer is Craig Tata (privacy@brainshark.com (mailto:privacy@brainshark.com))

Brainshark's address is:

Brainshark, Inc.
260 Charles Street - Suite 101
Waltham, MA 02453

Privacy Policy

VoiceVibes, Inc Privacy Policy

This Privacy Policy describes how VoiceVibes, Inc. ("VoiceVibes") may collect information from or about you when you visit our website and use our service. VoiceVibes values your privacy and is providing this Privacy Policy to explain what information we collect and how that information may be used by VoiceVibes when you interact with VoiceVibes online.

This Privacy Policy includes the following:

1. OUR COMMITMENT TO YOUR PRIVACY
2. THE INFORMATION AND DATA WE COLLECT
3. HOW WE USE YOUR DATA
4. WHAT DATA OR INFORMATION MAY BE SHARED WITH THIRD PARTIES
5. HOW LONG WE SAVE YOUR DATA
6. HOW TO EDIT OR MODIFY DATA
7. HOW TO CANCEL YOUR VOICEVIBES ACCOUNT
8. CHILDREN'S PRIVACY
9. INFORMATION SECURITY
10. ADDITIONAL INFORMATION FOR EU, UK AND SWITZERLAND BASED USERS
11. PRIVACY NOTICE FOR CALIFORNIA RESIDENTS
12. WHEN THE VOICEVIBES PRIVACY POLICY APPLIES/LINKS
13. CHANGES TO PRIVACY POLICY
14. ACCEPTANCE
15. CONTACT

1. OUR COMMITMENT TO YOUR PRIVACY

Introduction - Our goal at VoiceVibes is to help you achieve your goals of learning to communicate more effectively. As we continue to develop our service, we are committed to respecting your privacy and protecting your personal information. We have created our Privacy Policy to inform you about the types of personal information that we may collect from you and how it will be handled. Please take a few minutes to review our policy before using our service or submitting any personal information.

International Users - VoiceVibes is hosted and operated entirely in the United States

and is subject to United States law. Any personal information that you provide to VoiceVibes is being transferred to VoiceVibes solely in the United States and will be hosted on United States servers. You consent to the transfer of your personal information to the United States. If you are a visitor from the European Union, United Kingdom or Switzerland, please see "HOW WE HANDLE DATA FROM VISITORS FROM THE UNITED KINGDOM, SWITZERLAND OR ANY COUNTRY BELONGING TO THE EUROPEAN UNION," below.

2. THE INFORMATION AND DATA WE COLLECT

General Site Usage

When using the Website for information purposes only, i.e. when you do not provide us with any information, VoiceVibes only collects the personal data that your browser transmits to our server. If you wish to view our Website, VoiceVibes collects the following data, which is technically necessary for us to display our Website to you and to ensure stability and security (Legal basis is Art. 6 para. 1 sentence 1 lit. f GDPR):

- IP address,
- Date and time of the request,
- Time zone,
- Content of the request (specific page),
- Access status/HTTP status code,
- Amount of data transferred in each case,
- Website from which the request comes,
- Browser,
- Operating system and its interface,
- Language and version of the browser software.

In addition to the aforementioned data, cookies are stored on your computer when you use our Website. Cookies are small text files that are stored on your hard disk by the browser you use and through which certain information flows to the user that places the cookie. Cookies cannot run programs or transmit viruses to your computer. They serve to make the Internet more user-friendly and effective overall.

Use of cookies and HTML 5 Local Storage:

a) This Website uses the following types of cookies, the scope and functionality of which

are explained below:

- Transient cookies (see c),
- Persistent cookies (see d).

b) In addition to our use of cookies, this website also uses HTML 5 Local Storage to store website preferences and session information.
c) Transient cookies are deleted automatically when you close your browser. This includes session cookies, which store a so-called session ID that can assign different requests of your browser to the joint session. This will allow your computer to be recognized when you return to our Website. Session cookies are deleted when you log out or close your browser.
d) Persistent cookies and HTML 5 Local Storage are automatically deleted after a specified period, which may vary depending on the cookie or Local Storage setting. You can delete cookies and Local Storage at any time in the security settings of your browser.
e) You can configure your browser settings according to your wishes and refuse to accept HTML 5 Local Storage, third party cookies or any cookies, for example. Please note that, in this event, you may not be able to use all functions of our Website.

When You Create an Account - In order to access VoiceVibes' services, we require users to register with us. When you create an account with VoiceVibes, we ask for some personal information, including your name, email address, year of birth, etc.

Use of Collected Information - We use the information we collect in the following ways:

- To operate, maintain, and improve our services. For example, we can use audio recordings for internal R&D purposes to improve the quality of VoiceVibes' services.
- To create your account, identify you as a user, and customize VoiceVibes services for your account.
- To send you administrative communications. These may include administrative emails, confirmations, technical notices, surveys, updates, and security alerts.
- To respond to your comments and questions and provide you with user support.
- To process payments which you make to VoiceVibes.
- To protect, investigate, and deter against fraudulent, unauthorized, or illegal activity.

Email - Your email address will be your VoiceVibes account user name, which you will

use to log-on to your account. We do not display your email address to other users. Instead, others will see the name or nickname you enter in your profile settings.

Other Registration Information - No other registration information will be made public.

When You Add Information to Your Account - You can update your VoiceVibes account or add information to your account at any time. Whenever you add this type of information, we collect it and store it in your VoiceVibes account.

When You Use the Mobile App - You will be invited to download the VoiceVibes Recorder App and enter your username and password. This App enables you to record your speeches and upload them for analysis by the VoiceVibes service.

When You Upload Audio in Your VoiceVibes Account - When you upload your voice audio data, recorded through the mobile App, web browser, or by other means, the audio file will be transferred to our servers. This data is stored and used to provide the VoiceVibes service and is associated with your account. Each time an upload occurs, we log data about the transmission. Some examples of the log data are the sync time, date, and the IP address used when uploading.

When you Share your Audio File with an Instructor or a Peer - When your account is associated with an organization, access to your audio recordings, audio scores/ratings and associated metadata may be made available to instructors and administrators for that organization. See "What Data or Information May Be Shared with Third Parties," below.

When You Make Purchases Through Our Website - We do not view or store your credit card information. That information is handled by our third-party payment processor. If you are logged into your VoiceVibes account when you make a purchase through our website, we associate that order with your VoiceVibes account.

When You Contact Us for Help - Whenever you contact VoiceVibes for assistance, we collect your name and email address along with additional information you provide in your request so that we can provide you with adequate assistance and improve the VoiceVibes service. You can also contact VoiceVibes through public forums such as Facebook or Twitter, but we cannot guarantee or maintain the privacy of your

communications to us if you choose these public forums.

Information from Other Sources - We do not collect any information about you from other sources outside of your interactions with the VoiceVibes mobile App and/or service unless you or your organization have provided permission to do so.

3. HOW WE USE YOUR DATA

General Administration - We use the information that you share with us to provide you with new and improved services and to better understand your needs. For example, we use the information you provide for internal research and development, business decision making, website trend analysis, record keeping, demographic reporting, finalizing your registration, communication with you regarding service assistance, and notifying you about updates to our services and policies.

Speech Rating System - A large component to the VoiceVibes service is rating your voice recordings to assist you in your goal of more effective communication. The voice recordings that you upload to your VoiceVibes account will be rated through VoiceVibes software, and in rare cases may be rated by individuals against certain criteria. These individual raters will not access other personally identifiable information. Short samples from your speech that do not contain personally identifiable information (other than your voice characteristics) may be manually clipped and saved under an anonymous identification number. These audio samples may be made available to third-party raters via a VoiceVibes-hosted website or a third-party website. You may opt out of this individual rating service by contacting **privacyofficer@myvoicevibes.com**.

4. WHAT DATA OR INFORMATION MAY BE SHARED WITH THIRD PARTIES

Overview - We do not sell, trade, or otherwise transfer your personally identifiable information to third parties. This does not include, however, trusted third parties who assist us in operating our website, conducting our business, or servicing you, so long as those parties agree to keep your information confidential. In addition, we may also release your information when we believe that it is appropriate to comply with the law, enforce our website policies, or protect the rights, property, or safety of VoiceVibes, its users, or others.

Sharing with Your Group - In the event that your account is associated with an organization, access to your audio recordings, audio scores/ratings and associated metadata may be made available to instructors and administrators for that organization — for example, recordings in an account associated with a college or university may be visible to the relevant instructors. Additionally, when recordings are "shared" by you in the VoiceVibes application, this allows instructors and/or other VoiceVibes users in the same class or group to access them. Instructors and administrators may develop reports containing audio scores/ratings, your name, and associated metadata to determine trends and progress of the organization's VoiceVibes participants.

Third Party Channel-Partners – We may share information for research purposes. If you signed up through a link or site provided by a Channel Partner, such as Center for Creative Leadership (CCL), you may have executed terms that vary from this agreement. In some cases, the Channel Partner has been granted the right to own or use your data in different ways. To access your agreement, refer to your agreement with the third-party organization that provided your VoiceVibes account invite link.

Third-Party Agents - We may employ individuals or other companies to perform business functions on our behalf. These trusted entities may have access to information that is required to perform their services but are prohibited by contract and commitments to your confidentiality from utilizing the information for any other purpose. These types of services may include data analysis, transcription of audio recording, rating collection, payment processing, information technology and related infrastructure, email delivery, and other similar services.

Disclosure to Government Authorities, Etc. - We may share personal information as we believe necessary or appropriate (a) to comply with applicable laws; (b) to comply with lawful requests and legal process, including to respond to requests from public and government authorities to meet national security or law enforcement requirements; (c) to enforce our Policy; and (d) to protect our rights, privacy, safety or property, and/or that of you or others.

Mergers and Acquisitions - Circumstances may arise where for business reasons, we decide to sell, expand, merge, or otherwise reorganize our business in the United States or another country. A transaction like this may involve the disclosure of personally identifying information to prospective or actual purchasers and/or receiving such

information from sellers. It is our practice to seek appropriate protection for your information in these types of transactions, including notifying you if a different company will receive this information. Any successor in a merger or acquisition shall be bound by this Privacy Policy.

Third-Party Links - We may provide links to external websites in order to make certain content and services available to you. These websites are beyond our control and are not governed by our Privacy Policy. Therefore, we are not responsible for the privacy practices or the content of third party websites and cannot be responsible for the protection and privacy of any information you provide to these sites. When you leave the VoiceVibes website, we encourage you to read the privacy policy of any other website you visit, particularly websites that ask for your personal information.

Cookies - A cookie is a small file containing a string of characters that is stored on a user's hard drive. VoiceVibes may send one or more cookies to your computer in order to uniquely identify your browser. In general, cookies help us determine whether you have previously visited VoiceVibes' website and allow us to track the use of our website. Your VoiceVibes cookies will not contain any personally identifiable information whether you have registered or not.

Purpose - We use cookies to store your account information and the preferences you have made while using VoiceVibes. We may also use cookies to track the number of visitors to our website and to help us understand how visitors use the website.

Third-Party Cookies - Advertising partners may help VoiceVibes deliver interactive advertising, such as banner ads, and may also use their own cookies to better understand the types of advertising and promotions that are most appealing to our customers.

Disabling Cookies - While most web browsers automatically accept cookies by default, you may choose to disable or decline cookies from a particular website. Please be aware that if you disable all cookies or even just the cookies delivered by VoiceVibes, this may impact your ability to use our website as well as others.

Browser Controls for "Do Not Track" - Some newer browsers have "Do Not Track" (DNT) features. When engaged, most DNT features send a signal or preference to websites that

you do not want to be tracked. Those websites or their third-party advertisers or content providers may continue to engage in activity you may view as tracking, even after you use the DNT, depending on the websites' privacy practices. Because there is not yet a common understanding of how to interpret the DNT signal, VoiceVibes does not currently respond to the browser DNT signals. We continue to work with the online industry to define a common understanding of DNT signals and to remain compliant with industry standards.

Data That You Direct Us to Share - You can direct us to share data with other parties. For example, you may authorize us to send status updates to your Facebook or Twitter account or direct us to share data with your employer as part of a corporate training program. Once you direct us to share your data with a third party, that data is governed by the third-party's privacy policy.

5. HOW LONG WE SAVE YOUR DATA

Personally Identifiable Information - Your personally identifiable information shall be retained by the Company unless you request that it be deleted by contacting **privacyofficer@myvoicevibes.com**. Your information will only be used for Company research purposes to develop new and improved services and to better understand customers' needs.

Non-Personally Identifiable Information - We may retain and use non-personally identifiable information such as aggregate data, performance metrics, usage statistics and other data that has been anonymized.

6. HOW TO EDIT OR MODIFY DATA

Data that you provide to VoiceVibes through the website can be deleted from your account from the Manage tab. If you remove data from your account, it will no longer appear to you or others who use the VoiceVibes service. Backups of that data may remain associated with your VoiceVibes account and in our archive servers.

7. HOW TO CANCEL YOUR VOICEVIBES ACCOUNT

You can cancel your VoiceVibes account by sending an email titled "Request to Terminate my VoiceVibes Account" to privacyofficer@myvoicevibes.com. Upon any cancellation, your personally identifiable information shall be retained by the Company unless you request that it be deleted by contacting **privacyofficer@myvoicevibes.com**

8. CHILDREN'S PRIVACY

VoiceVibes is not directed at persons under the age of 13. We do not knowingly collect any personally identifiable information from children under the age of 13. If a parent or guardian becomes aware that their child has provided us with information without their consent, they should contact the VoiceVibes Privacy Officer at privacyofficer@myvoicevibes.com, and we will delete such information as soon as reasonably practicable.

9. INFORMATION SECURITY

Security Practices - We have incorporated security measures like password hashing and idle session logout to protect against the loss, misuse, and alteration of the information under our control. Further, only authorized affiliates, service providers, subsidiaries, and employees, who have agreed to keep the information on VoiceVibes secure and confidential, will have access to our information. While we will make every effort to ensure that the information you provide us will be kept secure, there is no way for us to absolutely guarantee the security of your personal information.

No Liability for Acts of Third Parties - VoiceVibes uses a combination of technical and administrative security controls to maintain the security of your data, exercising all reasonable efforts to safeguard the confidentiality of your personal information. However, transmissions protected by industry standard security technology and implemented by human beings cannot be made entirely secure. Consequently, VoiceVibes shall not be liable for unauthorized disclosure of personal information due to no fault of its own, including—but not limited to—errors in transmission and unauthorized acts of VoiceVibes staff and/or third parties.

10. ADDITIONAL INFORMATION FOR EU, UK AND SWITZERLAND BASED USERS

Data protection regulations in Europe require VoiceVibes to disclose additional information regarding Personal Data collected from European users, and to limit VoiceVibes' use of such information in specific ways. This section provides additional information applicable to European Personal Data, which may not apply to users in other geographies.

If you are accessing VoiceVibes from the United Kingdom, Switzerland or any country belonging to the European Union, please be advised that it is our policy and intent to adhere to the principles of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as amended (commonly known as the General Data Protection Regulations, or "GDPR") for your personal data that it receives from the United Kingdom, Switzerland or any country belonging to the European Union. Therefore, the following provisions shall apply to your personal information if you are accessing the VoiceVibes services from the United Kingdom, Switzerland or any country belonging to the European Union and, although the Privacy Policy, in whole, applies to everyone using VoiceVibes services, to the extent that the following provisions conflict with the provisions provided elsewhere in this Privacy Policy, the following provisions will apply to you.

VoiceVibes is not directed at persons under the age of 16 in the United Kingdom, Switzerland or any country belonging to the European Union, and we do not knowingly collect any personally identifiable information from such children under the age of 16. If you are aware of a user under the age of 16 using any VoiceVibes product or service, please contact us at **privacyofficer@myvoicevibes.com**. If a parent or guardian becomes aware that their child under the age of 16 has provided us with information without their consent, they should contact the VoiceVibes Privacy Officer at privacyofficer@myvoicevibes.com, and we will delete such information as soon as reasonably practicable.

Information on the collection of personal data

(1) Personal data are all data that make you personally identifiable, e.g. name, address, email addresses, user behaviour.

(2) When you contact us by e-mail or via a contact form, the data you provide (your email address, if applicable, your name and your telephone number) will be saved by us in order to answer your questions. VoiceVibes will delete the data collected in this context when its storage is no longer necessary or restrict the processing if statutory retention

obligations exist.
(3) If VoiceVibes makes use of contracted service providers for individual functions of our services or would like to use your data for advertising purposes, VoiceVibes will inform you in detail about the respective processes below. VoiceVibes does not directly collect sensitive personal information (e.g. information that reveals race, ethnic origin, political affiliations, etc.), but it is possible that you will provide such information in the content of your voice recordings.
(4) VoiceVibes will use personal information only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual. VoiceVibes will take reasonable steps to ensure that personal information is relevant to its intended use, accurate, complete, and current.

Your rights
(1) You have the following rights regarding personal data concerning you:

- Right of information,
- Right of correction or deletion,
- Right of limitation of processing,
- Right of opposition to the processing,
- Right of data portability.

(2) You also have the right to complain to a data protection supervisory authority about our processing of your personal data.

Data Portability
Upon request, VoiceVibe shall provide individuals with their personal data that has been provided to VoiceVibes in a structured, commonly used and machine-readable format.

Right to Erasure
Upon request, VoiceVibes shall delete an individual's personal information without undue delay; provided, however, VoiceVibes has the right to retain such personal information as may be necessary for (i) compliance with legal obligations or for a task carried out in the public interest; (ii) for reasons of public interest in the area of public health; (iii) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes if VoiceVibes takes appropriate measures for data minimization that no longer permits the identification of the individual; and (iv) for the establishment, exercise or defense of legal claims.

Termination/Deactivation

When you terminate or deactivate your VoiceVibes account, data that can identify you will be removed from the VoiceVibes service, and if you consented during sign-up, we can retain your data after your account has been closed, but you are also able to revoke this consent at any time, either before, during or after account closure.

Access and Correction

Upon request, VoiceVibes will grant individuals reasonable access to personal information that it holds about them. In addition, VoiceVibes will permit individuals to correct, amend, supplement or delete information that is demonstrated to be inaccurate or incomplete. VoiceVibes will notify any third party agent to whom the personal information has been disclosed that such personal information has been corrected, unless doing so proves to be impossible or involves disproportionate effort.

Use of social media plug-ins

(1) VoiceVibes currently uses the following social media plug-ins: Facebook, LinkedIn, Twitter, YouTube. VoiceVibes uses the so-called two-click solution. This means that when you visit our Website, no personal data is initially passed on to the providers of the plug-ins. You can recognise the provider of the plug-in by the marking on the box above its initial letter or the logo. VoiceVibes offers you the possibility to communicate directly with the provider of the plug-in via the button. Only if you click on the marked field and thereby activate it, the plug-in provider receives the information that you have accessed the corresponding Website of our online offer. In addition, the data mentioned in the section "Collection of personal data when you visit our Website" of this Privacy Policy will be transmitted. In the case of Facebook, the IP address is anonymised immediately after collection, according to the respective provider. By activating the plug-in, personal data is transferred from you to the respective plug-in provider and stored there. Since the plug-in provider collects data mainly via cookies, VoiceVibes recommends that you delete all cookies before clicking on the greyed-out box using your browser's security settings.

(2) VoiceVibes has no influence on the data collected and data processing processes, nor is VoiceVibes aware of the full extent of data collection, the purposes of processing, or the storage periods. VoiceVibes does not have information on the deletion of the data collected by the plug-in provider.

(3) The plug-in provider stores the data collected about you as user profiles and uses

these for the purposes of advertising, market research and/or demand-oriented design of its Website. Such an evaluation takes place in particular (also for non-logged-in users) for the representation of suitable advertisements and in order to inform other users of the social network about your activities on our Website. You have a right of objection to the creation of these user profiles, whereby you must contact the respective plug-in provider to exercise this right. Through the plug-ins, VoiceVibes offers you the ability to interact with social networks and other users, so that VoiceVibes can improve our service and make it more interesting for you as a user. The legal basis for the use of the plug-ins is Art. 6 para. 1 sentence 1 lit. f GDPR.

(4) The data is passed on regardless of whether you have an account with the plug-in provider and are logged in there. If you are logged in with the plug-in provider, your data collected with us will be directly assigned to your existing account with the plug-in provider. If you click the activated button and, for example, link the page, the plug-in provider also stores this information in your user account and shares it publicly with your contacts. VoiceVibes recommends that you log out regularly after using a social network, especially before activating the button, as this way you can avoid being assigned to your profile with the plug-in provider.

(5) Further information on the purpose and scope of data collection and its processing by the plug-in provider can be found in the privacy policy of these providers listed below. They will also provide you with further information about your rights in this regard and how to set options to protect your privacy.

(6) Addresses of the respective plug-in providers and URLs with their data protection information:

a) LinkedIn Corporation, 2029 Stierlin Court, Mountain View, California 94043, USA; **http://www.linkedin.com/legal/privacy-policy**. LinkedIn has submitted to the EU-US Privacy Shield, **https://www.privacyshield.gov/EU-US-Framework**.

b) Facebook Inc, 1601 S California Ave, Palo Alto, California 94304, USA; **http://www.facebook.com/policy.php**; further information on data collection: **http://www.facebook.com/help/186325668085084**, **http://www.facebook.com/about/privacy/your-info-on-other#applications**. Facebook has submitted to the EU-US Privacy Shield, **https://www.privacyshield.gov/EU-US-Framework**

c) *Twitter, Inc., 1355 Market St, Suite 900, San Francisco, California 94103, USA; https://twitter.com/privacy. Twitter* has submitted to the EU-US Privacy Shield, *https://www.privacyshield.gov/EU-US-Framework*.

d) YouTube LLC, 901 Cherry Ave., San Bruno, CA 94066, USA; **https://policies.google.com/privacy?hl=en&gl=en**.

Integration of YouTube videos

(1) VoiceVibes have integrated YouTube videos into our online website, which are stored on **http://www.YouTube.com** and can be played directly from our website. These are all integrated in the "extended data protection mode", i.e. no data about you as a user will be transmitted to YouTube if you do not play the videos. Only when you play the videos will the data referred to in paragraph 2 be transmitted. VoiceVibes has no influence on this data transmission.

(2) By visiting the Website, YouTube receives the information that you have accessed the corresponding subpage of our Website. In addition, the data mentioned in the section "Collection of personal data when you visit our Website" of this Privacy Policy will be transmitted. This does not depend on whether YouTube provides a user account through which you are logged in or whether no user account exists. If you are logged into Google, your information will be directly associated with your account. If you do not wish to be associated with your profile on YouTube, you must log out before activating the button. YouTube stores your data as user profiles and uses them for purposes of advertising, market research and/or demand-oriented design of its website. Such evaluation takes place in particular (even for non-logged-in users) to provide demand-oriented advertising and to inform other users of the social network about your activities on our Website. You have the right to object to the creation of these user profiles, but you must contact YouTube to exercise this right.

(3) Further information on the purpose and scope of data collection and processing by YouTube can be found in YouTube's privacy policy. There you will also find further information about your rights and how to set options to protect your privacy. Google also processes your personal data in the USA and has submitted to the EU-US Privacy Shield, **https://www.privacyshield.gov/EU-US-Framework**.

Choice.

You can contact us any time to opt-out of (a) promotional communications, or (b) any new processing of your personal information that we may carry out beyond the original purpose, or (c) the transfer of your personal information outside the United Kingdom, Switzerland or any country of the European Union (opting out of this subsection (c) will cause VoiceVibes' services to be ineffective upon opt-out).

Transfers to Agents.

VoiceVibes will obtain assurances from its agents that they will safeguard personal

information consistently with GDPR, including providing the same level of protection as is required under GDPR. Where VoiceVibes has knowledge that an agent is using or disclosing personal information in a manner contrary to GDPR, VoiceVibes will take reasonable steps to prevent or stop the use or disclosure.

Security.
VoiceVibes will take reasonable precautions to protect personal information in its possession from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

Enforcement.
VoiceVibes will conduct compliance audits of its relevant privacy practices to verify adherence to this Privacy Policy. Any employee that VoiceVibes determines is in violation of this Privacy Policy will be subject to disciplinary action up to and including termination of employment.

Retention of Personal Information.
If your VoiceVibes account becomes inactive because it was not timely renewed, and you have not opted in to permit us to retain your personal information, we will keep your personal information for a period of three months prior to beginning the process of deleting it. This will enable us to promptly reactivate your account in the event you renew during the initial three month period. Once the process of deleting your personal information has begun, it is possible that it may take up to an additional three months for all copies of your personal information to be removed from all of VoiceVibes' systems, backups, log files, and archives.

Objection or revocation of the processing of your data
(1) If you have given your consent to the processing of your data, you can revoke it at any time. Such revocation affects the lawfulness of processing your personal data after you have made it known to us.
(2) If we base the processing of your personal data on the weighing of interests, you may object to the processing. This is the case in particular if processing is not necessary to fulfil a contract with you, which we explain in the following description of the functions. When you do object, we would ask you to explain the reasons why we should not process your personal data. In the event of a justified objection, we will examine the situation and either stop or adjust data processing, or point out to you our compelling

reasons worthy of protection, on the basis of which we will continue processing.
(3) Of course, you can object to the processing of your personal data for the purposes of advertising and data analysis at any time. You can inform us about your contradiction using the following contact data:

VoiceVibes, Inc.
7224 Shub Farm Rd.
Marriottsville, MD 21104
USA
email: privacyofficer@myvoicevibes.com

Contact/Dispute Resolution
Any questions or concerns regarding the use or disclosure of, or any of your rights regarding, your personal information should be directed to the VoiceVibes Privacy Officer at privacyofficer@myvoicevibes.com. VoiceVibes will investigate and attempt to resolve complaints and disputes regarding use and disclosure of personal information by reference to the principles contained in this Privacy Policy.

11. PRIVACY NOTICE FOR CALIFORNIA RESIDENTS

Effective Date: January 1, 2020
Last Reviewed on: February 22, 2021
This Privacy Notice for California Residents supplements the information contained in Bigtincan's Privacy policy and applies solely to all visitors, users, and others who reside in the State of California ("consumers" or "you"). We adopt this notice to comply with the California Consumer Privacy Act of 2018 (CCPA) and any terms defined in the CCPA have the same meaning when used in this notice.

Information We CollectOur Website collects information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device ("personal information"). In particular, Bigtincan's website, **https://www.bigtincan.com/** ("Website"), has collected the following categories of personal information from its consumers in California within the last twelve (12) months:

A. Identifiers. Examples: Name, email address, telephone number, Internet Protocol

address. Collected: YES

B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)). Examples: Name, email address, telephone number. Some personal information included in this category may overlap with other categories. Collected: YES

C. Protected classification characteristics under California or federal law. Examples: Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information). Collected: OPTIONAL

D. Commercial information. Examples: Records of Bigtincan products or services considered on our website. Collected: YES

E. Biometric information. Examples: Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data. Collected: YES

F. Internet or other similar network activity. Examples: Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement. Collected: YES

G. Geolocation data. Examples: Physical location or movements. Collected: YES

H. Sensory data. Examples: Audio, electronic, visual, thermal, olfactory, or similar information. Collected: YES

I. Professional or employment-related information. Examples: Current or past job history or performance evaluations. Collected: NO

J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)). Examples: Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records. Collected: YES

K. Inferences drawn from other personal information. Examples: Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. Collected: YES

Personal information does not include:

- Publicly available information from government records.
- Deidentified or aggregated consumer information.
- Information excluded from the CCPA's scope, like:
- Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data;
- Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

Bigtincan obtains the categories of personal information listed above from the following categories of sources:

- Directly from you. For example, from forms you complete.
- Indirectly from you. For example, from observing your actions on our Website.

Use of Personal Information We may use, or disclose the personal information we collect for one or more of the following business purposes:

- To fulfill or meet the reason you provided the information. For example, if you share your name and contact information or ask a question about our products or services, we will use that personal information to respond to your inquiry.
- To provide, support, personalize, and develop our Website, products, and services.
- To process your information requests.
- To provide you with support and to respond to your inquiries, including to investigate and address your concerns and monitor and improve our responses.
- To personalize your Website experience and to deliver content and product and service offerings relevant to your interests, including targeted offers and ads through our Website, third-party sites, and via email or text message (with your consent, where required by law).
- To help maintain the safety, security, and integrity of our Website, products and services, databases and other technology assets, and business.
- For testing, research, analysis, and product development, including to develop and improve our Website, products, and services.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.

- As described to you when collecting your personal information or as otherwise set forth in the CCPA.

Bigtincan will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sharing Personal InformationBigtincan may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract.

We share your personal information with the following categories of third parties:

- Service providers.
- Data aggregators.

Disclosures of Personal Information for a Business Purpose

In the preceding twelve (12) months, Company has disclosed the following categories of personal information for a business purpose:

[Category A: Identifiers.]

[Category B: California Customer Records personal information categories.]

[Category D: Commercial information.]

[Category F: Internet or other similar network activity.]

[Category G: Geolocation data.]

We disclose your personal information for a business purpose to the following categories of third parties:

- Service providers.
- Data aggregators

Sales of Personal Information

In the preceding twelve (12) months, Company has not sold personal information

Your Rights and ChoicesThe CCPA provides consumers (California residents) with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights.

Access to Specific Information and Data Portability Rights

You have the right to request that Bigtincan disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request (see *Exercising Access, Data Portability, and Deletion Rights*), we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting that personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you (also called a data portability request).
- If we disclosed your personal information for a business purpose, providing disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.

Deletion Request Rights

You have the right to request that Bigtincan delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request (see *Exercising Access, Data Portability, and Deletion Rights*), we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

9. Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
10. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
11. Debug products to identify and repair errors that impair existing intended functionality.
12. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
13. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 *et. seq.*).
14. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
15. Comply with a legal, regulatory or other governmental obligation.
16. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

Exercising Access, Data Portability, and Deletion Rights

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by either:

- Phone: (617) 981-7557
- Email: **privacy@bigtincan.com**
- Physical Address: Bigtincan Mobile Pty Ltd, Level 6, 338 Pitt Street, Sydney, New South Wales, Australia 2000.

Only you, or a person registered with the California Secretary of State that you authorize to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you.

Making a verifiable consumer request does not require you to create an account with us. However, we do consider requests made through your password protected account sufficiently verified when the request relates to personal information associated with that specific account.

We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Response Timing and Format

We endeavor to respond to a verifiable consumer request within thirty (30) days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing.

If you have an account with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option.

Any disclosures we provide will only cover the 12-month period preceding the verifiable

consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.
We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.
Other California Privacy RightsCalifornia's "Shine the Light" law (Civil Code Section § 1798.83) permits users of our Website that are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please send an email to **privacy@bigtincan.com** or write us at:
Attn: Bigtincan Privacy officer
Phone: (617) 981-7557
Email: **privacy@bigtincan.com**
Address: Bigtincan Mobile Pty Ltd, Level 6, 338 Pitt Street, Sydney, New South Wales, Australia 2000

12. WHEN THE VOICEVIBES PRIVACY POLICY APPLIES/LINKS

The VoiceVibes Privacy Policy applies to all of our services, products, mobile applications, and our website.

If you use external links that are offered on our website, this Privacy Policy does not extend to those links. When VoiceVibes provide links, we endeavour to ensure that they also comply with our Privacy Policy and security standards. However, we have no influence on compliance with privacy policy and security regulations by other providers and websites. Therefore, please also inform yourself about the privacy policies provided on the websites of other providers.

13. CHANGES TO PRIVACY POLICY

The use of the information that we gather is subject to the Privacy Policy in effect at the time the information is submitted. We reserve the right, however, to update this Privacy Policy at any time. We will post any Privacy Policy changes on this page, and if the changes are more significant, we will provide a more prominent notice (including, for

certain services, email notification of privacy policy changes to registered users and/or display notifications on the VoiceVibes website). We will not reduce your rights under this Privacy Policy without your explicit consent. We will also keep prior versions of the Privacy Policy in an archive for your review.

14. ACCEPTANCE

When a significant change to this Privacy Policy goes into effect, registered users will be prompted to review the changes and to select whether they accept or do not accept VoiceVibes' planned updates.

15. CONTACT US

You can contact us with any questions or comments at:
privacyofficer@myvoicevibes.com.