

PRIVACY NOTICE

Last updated [\[Date\]](#)

This privacy notice for [\[Company Name\]](#) (doing business as [\[Company Short Name\]](#)) ("we," "us," or "our"), describes how and why we might collect, store, use, and/or share ("process") your information when you use our services ("Services"), such as when you:

- Visit our website at [\[Website URL\]](#), or any website of ours that links to this privacy notice
- [\[Download and use our application\(s\), such as our mobile application – \[Mobile App Name\], \[our Facebook application – \[Facebook App Name\],\] or any other application of ours that links to this privacy notice\]](#)
- Engage with us in other related ways – including any sales, marketing, or events

Questions or concerns? Reading this privacy notice will help you understand your privacy rights and choices. If you do not agree with our policies and practices, please do not use our Services. If you still have any questions or concerns, please contact us at [\[Email Address\]](#).

This privacy policy was created by Termly's [Privacy Policy Generator](#).

SUMMARY OF KEY POINTS

This summary provides key points from our privacy notice, but you can find out more details about any of these topics by clicking the link following each key point or by using our [table of contents](#) below to find the section you are looking for.

What personal information do we process? When you visit, use, or navigate our Services, we may process personal information depending on how you interact with us and the Services, the choices you make, and the products and features you use. Learn more about [personal information you disclose to us](#).

Do we process any sensitive personal information? [\[We do not process sensitive personal information. / We may process sensitive personal information when necessary with your consent or as otherwise permitted by applicable law. Learn more about sensitive information we process.\]](#)

Do we receive any information from third parties? We may receive information from public databases, marketing partners, social media platforms, and other outside sources. Learn more about [information collected from other sources](#).

How do we process your information? We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent. We process your information only when we have a valid legal reason to do so. Learn more about [how we process your information](#).

In what situations and with which types of parties do we share personal information? We may share information in specific situations and with specific categories of third parties. Learn more about [when and with whom we share your personal information](#).

How do we keep your information safe? We have organizational and technical processes and procedures in place to protect your personal information. However, no electronic transmission over the internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security and improperly collect, access, steal, or modify your information. Learn more about [how we keep your information safe](#).

What are your rights? Depending on where you are located geographically, the applicable privacy law may mean you have certain rights regarding your personal information. Learn more about [your privacy rights](#).

How do I exercise my rights? The easiest way to exercise your rights is by filling out our data subject access request form available here: [\[DSAR Form URL\]](#), or by contacting us. We will consider and act upon any request in accordance with applicable data protection laws.

Want to learn more about what we do with any information we collect? [Review the privacy notice in full](#).

TABLE OF CONTENTS

[1. WHAT INFORMATION DO WE COLLECT?](#)

[2. HOW DO WE PROCESS YOUR INFORMATION?](#)

[3. WHAT LEGAL BASES DO WE RELY ON TO PROCESS YOUR PERSONAL INFORMATION?](#)

[4. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?](#)

[5. WHAT IS OUR STANCE ON THIRD-PARTY WEBSITES?](#)

[6. DO WE USE COOKIES AND OTHER TRACKING TECHNOLOGIES?](#)

[7. HOW DO WE HANDLE YOUR SOCIAL LOGINS?](#)

[8. IS YOUR INFORMATION TRANSFERRED INTERNATIONALLY?](#)

[9. HOW LONG DO WE KEEP YOUR INFORMATION?](#)

[10. HOW DO WE KEEP YOUR INFORMATION SAFE?](#)

[11. DO WE COLLECT INFORMATION FROM MINORS?](#)

[12. WHAT ARE YOUR PRIVACY RIGHTS?](#)

[13. CONTROLS FOR DO-NOT-TRACK FEATURES](#)

[14. DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?](#)

[15. DO OTHER REGIONS HAVE SPECIFIC PRIVACY RIGHTS?](#)

[16. DO WE MAKE UPDATES TO THIS NOTICE?](#)

[17. HOW CAN YOU CONTACT US ABOUT THIS NOTICE?](#)

[18. HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?](#)

1. WHAT INFORMATION DO WE COLLECT?

Personal information you disclose to us

In Short: We collect personal information that you provide to us.

We collect personal information that you voluntarily provide to us when you [\[register on the Services,\]](#) express an interest in obtaining information about us or our products and Services, when you participate in activities on the Services, or otherwise when you contact us.

Personal Information Provided by You. The personal information that we collect depends on the context of your interactions with us and the Services, the choices you make, and the products and features you use. The personal information we collect may include the following:

- [\[Personal Info Collected\]](#)
- [\[Personal Info Collected\]](#)
- [\[Personal Info Collected\]](#)

Sensitive Information. [\[We do not process sensitive information. / When necessary, with your consent or as otherwise permitted by applicable law, we process the following categories of sensitive information:](#)

- [\[Sensitive Info Collected\]](#)
- [\[Sensitive Info Collected\]](#)
- [\[Sensitive Info Collected\]\]](#)

Payment Data. We may collect data necessary to process your payment if you make purchases, such as your payment instrument number (such as a credit card number), and the security code associated with your payment instrument. All payment data is stored by [\[Vendor Name\]](#). You may find their privacy notice link(s) here: [\[Vendor Privacy Policy\]](#).

Social Media Login Data. We may provide you with the option to register with us using your existing social media account details, like your Facebook, Twitter, or other social media account. If you choose to register in this way, we will collect the information described in the section called "[HOW DO WE HANDLE YOUR SOCIAL LOGINS?](#)" below.

[Application Data. If you use our application(s), we also may collect the following information if you choose to provide us with access or permission:

- **Geolocation Information.** We may request access or permission to track location-based information from your mobile device, either continuously or while you are using our mobile application(s), to provide certain location-based services. If you wish to change our access or permissions, you may do so in your device's settings.
- **Mobile Device Access.** We may request access or permission to certain features from your mobile device, including your mobile device's bluetooth, calendar, camera, own, and other features. If you wish to change our access or permissions, you may do so in your device's settings.
- **Mobile Device Data.** We automatically collect device information (such as your mobile device ID, model, and manufacturer), operating system, version information and system configuration information, device and application identification numbers, browser type and version, hardware model Internet service provider and/or mobile carrier, and Internet Protocol (IP) address (or proxy server). If you are using our application(s), we may also collect information about the phone network associated with your mobile device, your mobile device's operating system or platform, the type of mobile device you use, your mobile device's unique device ID, and information about the features of our application(s) you accessed.
- **Push Notifications.** We may request to send you push notifications regarding your account or certain features of the application(s). If you wish to opt out from receiving these types of communications, you may turn them off in your device's settings.

This information is primarily needed to maintain the security and operation of our application(s), for troubleshooting, and for our internal analytics and reporting purposes.]

All personal information that you provide to us must be true, complete, and accurate, and you must notify us of any changes to such personal information.

Information automatically collected

In Short: Some information — such as your Internet Protocol (IP) address and/or browser and device characteristics — is collected automatically when you visit our Services.

We automatically collect certain information when you visit, use, or navigate the Services. This information does not reveal your specific identity (like your name or contact information) but may include device and usage information, such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, country, location, information about how and when you use our Services, and other technical information. This information is primarily needed to maintain the security and operation of our Services, and for our internal analytics and reporting purposes.

Like many businesses, we also collect information through cookies and similar technologies. You can find out more about this in our Cookie Notice: [\[Cookie Notice URL\]](#).

The information we collect includes:

- *Log and Usage Data.* Log and usage data is service-related, diagnostic, usage, and performance information our servers automatically collect when you access or use our Services and which we record in log files. Depending on how you interact with us, this log data may include your IP address, device information, browser type, and settings and information about your activity in the Services (such as the date/time stamps associated with your usage, pages and files viewed, searches, and other actions you take such as which features you use), device event information (such as system activity, error reports (sometimes called "crash dumps"), and hardware settings).
- *Device Data.* We collect device data such as information about your computer, phone, tablet, or other device you use to access the Services. Depending on the device used, this device data may include information such as your IP address (or proxy server), device and application identification numbers, location, browser type, hardware model, Internet service provider and/or mobile carrier, operating system, and system configuration information.
- *Location Data.* We collect location data such as information about your device's location, which can be either precise or imprecise. How much information we collect depends on the type and settings of the device you use to access the Services. For example, we may use GPS and other technologies to collect geolocation data that tells us your current location (based on your IP address). You can opt out of allowing us to collect this information either by refusing access to the information or by disabling your Location setting on your device. However, if you choose to opt out, you may not be able to use certain aspects of the Services.
- [\[Other\]](#)

Information collected from other sources

In Short: We may collect limited data from public databases, marketing partners, social media platforms, and other outside sources.

In order to enhance our ability to provide relevant marketing, offers, and services to you and update our records, we may obtain information about you from other sources, such as public databases, joint marketing partners, affiliate programs, data providers, social media platforms, and from other third parties. This information includes mailing addresses, job titles, email addresses, phone numbers, intent data (or user behavior data), Internet Protocol (IP) addresses, social media profiles, social media URLs, and custom profiles, for purposes of targeted advertising and event promotion. If you interact with us on a social media platform using your social media account (e.g., Facebook or Twitter), we receive personal information about you such as your name, email address, and gender. Any personal information that we collect from your social media account depends on your social media account's privacy settings.

[Information collected when you use our Facebook application(s). We by default access your Facebook basic account information, including your name, email, gender, birthday, current city, and profile picture URL, as well as other information that you choose to make public. We may also request access to other permissions related to your account, such as friends, check-ins, and likes, and you may choose to grant or deny us access to each individual permission. For more information regarding Facebook permissions, refer to the [Facebook Permissions Reference page](#).]

2. HOW DO WE PROCESS YOUR INFORMATION?

In Short: We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent.

We process your personal information for a variety of reasons, depending on how you interact with our Services, including:

- **To facilitate account creation and authentication and otherwise manage user accounts.** We may process your information so you can create and log in to your account, as well as keep your account in working order.
- **To deliver and facilitate delivery of services to the user.** We may process your information to provide you with the requested service.
- **To respond to user inquiries/offer support to users.** We may process your information to respond to your inquiries and solve any potential issues you might have with the requested service.
- **To send administrative information to you.** We may process your information to send you details about our products and services, changes to our terms and policies, and other similar information.

- **To fulfill and manage your orders.** We may process your information to fulfill and manage your orders, payments, returns, and exchanges made through the Services.
- **To enable user-to-user communications.** We may process your information if you choose to use any of our offerings that allow for communication with another user.
- **To request feedback.** We may process your information when necessary to request feedback and to contact you about your use of our Services.
- **To send you marketing and promotional communications.** We may process the personal information you send to us for our marketing purposes, if this is in accordance with your marketing preferences. You can opt out of our marketing emails at any time. For more information, see "[WHAT ARE YOUR PRIVACY RIGHTS?](#)" below).
- **To deliver targeted advertising to you.** We may process your information to develop and display personalized content and advertising tailored to your interests, location, and more. For more information see our Cookie Notice: [\[Cookie Notice URL\]](#).
- **To protect our Services.** We may process your information as part of our efforts to keep our Services safe and secure, including fraud monitoring and prevention.
- **To identify usage trends.** We may process information about how you use our Services to better understand how they are being used so we can improve them.
- **To determine the effectiveness of our marketing and promotional campaigns.** We may process your information to better understand how to provide marketing and promotional campaigns that are most relevant to you.
- **To save or protect an individual's vital interest.** We may process your information when necessary to save or protect an individual's vital interest, such as to prevent harm.
- [\[Other\]](#)

3. WHAT LEGAL BASES DO WE RELY ON TO PROCESS YOUR INFORMATION?

In Short: We only process your personal information when we believe it is necessary and we have a valid legal reason (i.e., legal basis) to do so under applicable law, like with your consent, to comply with laws, to provide you with services to enter into or fulfill our contractual obligations, to protect your rights, or to fulfill our legitimate business interests.

If you are located in the EU or UK, this section applies to you.

The General Data Protection Regulation (GDPR) and UK GDPR require us to explain the valid legal bases we rely on in order to process your personal information. As such, we may rely on the following legal bases to process your personal information:

- **Consent.** We may process your information if you have given us permission (i.e., consent) to use your personal information for a specific purpose. You can withdraw your consent at any time. Learn more about [withdrawing your consent](#).
- **Performance of a Contract.** We may process your personal information when we believe it is necessary to fulfill our contractual obligations to you, including providing our Services or at your request prior to entering into a contract with you.
- **Legitimate Interests.** We may process your information when we believe it is reasonably necessary to achieve our legitimate business interests and those interests do not outweigh your interests and fundamental rights and freedoms. For example, we may process your personal information for some of the purposes described in order to:
 - Send users information about special offers and discounts on our products and services
 - Develop and display personalized and relevant advertising content for our users
 - Analyze how our Services are used so we can improve them to engage and retain users
 - Support our marketing activities
 - Diagnose problems and/or prevent fraudulent activities
 - Understand how our users use our products and services so we can improve user experience
 - [\[Other\]](#)
- **Legal Obligations.** We may process your information where we believe it is necessary for compliance with our legal obligations, such as to cooperate with a law enforcement body or regulatory agency, exercise or defend our legal rights, or disclose your information as evidence in litigation in which we are involved.
- **Vital Interests.** We may process your information where we believe it is necessary to protect your vital interests or the vital interests of a third party, such as situations involving potential threats to the safety of any person.

In legal terms, we are generally the “data controller” under European data protection laws of the personal information described in this privacy notice, since we determine the means and/or purposes of the data processing we perform. This privacy notice does not apply to the personal information we process as a “data processor” on behalf of our customers. In those situations, the customer that we provide services to and with whom we have entered into a data processing agreement is the “data controller” responsible for your personal information, and we merely process your information on their behalf in accordance with your instructions. If you want to know more about our customers' privacy practices, you should read their privacy policies and direct any questions you have to them.

If you are located in Canada, this section applies to you.

We may process your information if you have given us specific permission (i.e., express consent) to use your personal information for a specific purpose, or in situations where your permission can be inferred (i.e., implied consent). You can withdraw your consent at any time. Click [here](#) to learn more.

In some exceptional cases, we may be legally permitted under applicable law to process your information without your consent, including, for example:

- If collection is clearly in the interests of an individual and consent cannot be obtained in a timely way
- For investigations and fraud detection and prevention
- For business transactions provided certain conditions are met
- If it is contained in a witness statement and the collection is necessary to assess, process, or settle an insurance claim
- For identifying injured, ill, or deceased persons and communicating with next of kin
- If we have reasonable grounds to believe an individual has been, is, or may be victim of financial abuse
- If it is reasonable to expect collection and use with consent would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province
- If disclosure is required to comply with a subpoena, warrant, court order, or rules of the court relating to the production of records
- If it was produced by an individual in the course of their employment, business, or profession and the collection is consistent with the purposes for which the information was produced
- If the collection is solely for journalistic, artistic, or literary purposes
- If the information is publicly available and is specified by the regulations

4. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?

In Short: We may share information in specific situations described in this section and/or with the following categories of third parties.

Vendors, Consultants, and Other Third-Party Service Providers. We may share your data with third-party vendors, service providers, contractors, or agents (“**third parties**”) who perform services for us or on our behalf and require access to such information to do that work. We have contracts in place with our third parties, which are designed to help safeguard your personal information. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will also not share your personal information with any organization apart from us. They also commit to protect the data they hold on our behalf and to retain it for the period we instruct. The categories of third parties we may share personal information with are as follows:

- Ad Networks
- Affiliate Marketing Programs
- Cloud Computing Services
- Communication & Collaboration Tools
- Data Analytics Services
- Data Storage Service Providers
- Finance & Accounting Tools
- Government Entities
- Order Fulfillment Service Providers
- Payment Processors
- Performance Monitoring Tools
- Product Engineering & Design Tools
- Retargeting Platforms
- Sales & Marketing Tools
- Social Networks
- Testing Tools
- User Account Registration & Authentication Services
- Website Hosting Service Providers
- [\[Other\]](#)

We also may need to share your personal information in the following situations:

- **Business Transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.
- **When we use Google Analytics.** We may share your information with Google Analytics to track and analyze the use of the Services. The Google Analytics Advertising Features that we may use include: [\[List Features\]](#). To opt out of being tracked by Google Analytics across the Services, visit <https://tools.google.com/dlpage/gaoptout>. You can opt out of Google Analytics Advertising Features through [Ads Settings](#) and Ad Settings for mobile apps. Other opt out means include <http://optout.networkadvertising.org/> and <http://www.networkadvertising.org/mobile-choice>. For more information on the privacy practices of Google, please visit the [Google Privacy & Terms page](#).
- **When we use Google Maps Platform APIs.** We may share your information with certain Google Maps Platform APIs (e.g., Google Maps API, Places API). To find out more about Google's Privacy Policy, please refer to this [link](#). We use certain Google Maps Platform APIs to retrieve certain information when you make location-specific requests. This includes: [\[List of Information Collected\]](#), and other similar information. A full list of what we use information for can be found in this section and in the previous section titled "[HOW DO WE PROCESS YOUR INFORMATION?](#)" [\[We](#)

obtain and store on your device ("cache") your location for [#] months. You may revoke your consent anytime by contacting us at the contact details provided at the end of this document.]

The Google Maps Platform APIs that we use store and access cookies and other information on your devices. If you are a user currently in the European Economic Area (EU countries, Iceland, Liechtenstein and Norway) or the United Kingdom, please take a look at our Cookie Notice, which can be found at this link: [\[Cookie Notice URL\]](#).

- **Affiliates.** We may share your information with our affiliates, in which case we will require those affiliates to honor this privacy notice. Affiliates include our parent company and any subsidiaries, joint venture partners, or other companies that we control or that are under common control with us.
- **Business Partners.** We may share your information with our business partners to offer you certain products, services, or promotions.
- **Other Users.** When you share personal information (for example, by posting comments, contributions, or other content to the Services) or otherwise interact with public areas of the Services, such personal information may be viewed by all users and may be publicly made available outside the Services in perpetuity. If you interact with other users of our Services and register for our Services through a social network (such as Facebook), your contacts on the social network will see your name, profile photo, and descriptions of your activity. Similarly, other users will be able to view descriptions of your activity, communicate with you within our Services, and view your profile.
- **[Offer Wall.** Our application(s) may display a third-party hosted "offer wall." Such an offer wall allows third-party advertisers to offer virtual currency, gifts, or other items to users in return for the acceptance and completion of an advertisement offer. Such an offer wall may appear in our application(s) and be displayed to you based on certain data, such as your geographic area or demographic information. When you click on an offer wall, you will be brought to an external website belonging to other persons and will leave our application(s). A unique identifier, such as your user ID, will be shared with the offer wall provider in order to prevent fraud and properly credit your account with the relevant reward.]

5. WHAT IS OUR STANCE ON THIRD-PARTY WEBSITES?

In Short: We are not responsible for the safety of any information that you share with third parties that we may link to or who advertise on our Services, but are not affiliated with, our Services.

The Services, [\[including our offer wall\]](#), may link to third-party websites, online services, or mobile applications and/or contain advertisements from third parties that are not affiliated with us and which may link to other websites, services, or applications. Accordingly, we do not make any guarantee regarding any such third parties, and we will not be liable for any loss or damage caused by the use of

such third-party websites, services, or applications. The inclusion of a link towards a third-party website, service, or application does not imply an endorsement by us. We cannot guarantee the safety and privacy of data you provide to any third parties. Any data collected by third parties is not covered by this privacy notice. We are not responsible for the content or privacy and security practices and policies of any third parties, including other websites, services, or applications that may be linked to or from the Services. You should review the policies of such third parties and contact them directly to respond to your questions.

6. DO WE USE COOKIES AND OTHER TRACKING TECHNOLOGIES?

In Short: We may use cookies and other tracking technologies to collect and store your information.

We may use cookies and similar tracking technologies (like web beacons and pixels) to access or store information. Specific information about how we use such technologies and how you can refuse certain cookies is set out in our Cookie Notice: [\[Cookie Notice URL\]](#).

7. HOW DO WE HANDLE YOUR SOCIAL LOGINS?

In Short: If you choose to register or log in to our Services using a social media account, we may have access to certain information about you.

Our Services offer you the ability to register and log in using your third-party social media account details (like your Facebook or Twitter logins). Where you choose to do this, we will receive certain profile information about you from your social media provider. The profile information we receive may vary depending on the social media provider concerned, but will often include your name, email address, friends list, and profile picture, as well as other information you choose to make public on such a social media platform. [\[If you log in using Facebook, we may also request access to other permissions related to your account, such as your friends, check-ins, and likes, and you may choose to grant or deny us access to each individual permission.\]](#)

We will use the information we receive only for the purposes that are described in this privacy notice or that are otherwise made clear to you on the relevant Services. Please note that we do not control, and are not responsible for, other uses of your personal information by your third-party social media provider. We recommend that you review their privacy notice to understand how they collect, use and share your personal information, and how you can set your privacy preferences on their sites and apps.

8. IS YOUR INFORMATION TRANSFERRED INTERNATIONALLY?

In Short: We may transfer, store, and process your information in countries other than your own.

Our servers are located in [\[Country\]](#). If you are accessing our Services from outside [\[Country\]](#), please be aware that your information may be transferred to, stored, and processed by us in our facilities and by those third parties with whom we may share your personal information (see "[WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?](#)" above), in [\[Country\]](#), and other countries.

If you are a resident in the European Economic Area (EEA), United Kingdom (UK), or Switzerland, then these countries may not necessarily have data protection laws or other similar laws as comprehensive as those in your country. However, we will take all necessary measures to protect your personal information in accordance with this privacy notice and applicable law.

European Commission's Standard Contractual Clauses:

We have implemented measures to protect your personal information, including by using the European Commission's Standard Contractual Clauses for transfers of personal information between our group companies and between us and our third-party providers. These clauses require all recipients to protect all personal information that they process originating from the EEA or UK in accordance with European data protection laws and regulations. Our Data Processing Agreements that include Standard Contractual Clauses are available here: [\[Standard Contractual Clauses URL\]](#). We have implemented similar appropriate safeguards with our third-party service providers and partners and further details can be provided upon request.

Binding Corporate Rules:

These include a set of Binding Corporate Rules ("BCRs") established and implemented by us. Our BCRs have been recognized by EEA and UK data protection authorities as providing an adequate level of protection to the personal information we process internationally. You can find a copy of our BCRs here: [\[BCRs URL\]](#).

[\[EU-US\]](#) and [\[Swiss-US\]](#) Privacy Shield Framework[\[s\]](#)

We and the following entities and subsidiaries: [\[List of Entities/Subsidiaries\]](#) comply with the [\[EU-US\]](#) and [\[Swiss-US\]](#) Privacy Shield Framework[\[s\]](#) as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from [\[the European Union \(EU\)\]](#), [\[the UK\]](#), and [\[Switzerland\]](#) to the United States. Although Privacy Shield is no longer considered a valid transfer mechanism for the purposes of [\[EU\]](#) and [\[Swiss\]](#) data protection law, in light of the judgment of the Court of Justice of the European Union in Case C-311/18 and opinion of the Federal Data Protection

and Information Commissioner of Switzerland dated 8 September 2020, we will continue to comply with the principles of the [\[EU-US\]](#) and [\[Swiss-US\]](#) Privacy Shield Framework[s]. Learn more about the [Privacy Shield program](#). To view our certification, please visit [\[Privacy Shield Certification URL\]](#).

We adhere to and comply with the Privacy Shield Principles when processing personal information from [\[the EU\]](#), [\[UK\]](#), or [\[Switzerland\]](#). If we have received your personal information in the United States and subsequently transfer that information to a third party acting as our agent, and such third party agent processes your personal information in a manner inconsistent with the Privacy Shield Principles, we will remain liable unless we can prove we are not responsible for the event giving rise to the damage.

With respect to personal information received or transferred pursuant to the Privacy Shield Framework[s], we are subject to the investigatory and enforcement powers of the US Federal Trade Commission ("FTC"). In certain situations, we may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

If you have any questions or concerns relating to our Privacy Shield certification, please write to us at the contact details below. We commit to resolving any complaints or disputes about our collection and use of your personal information under the Privacy Shield. [\[However, if you have an unresolved complaint in connection with our certification, we commit to cooperating with the panel established by \[the EU data protection authorities \(DPAs\)\], \[the UK Information Commissioner\], and \[the Swiss Federal Data Protection and Information Commissioner\], as applicable, and to comply with the advice given by them in respect of the complaint. See the following \[list of EU DPAs\]\(#\). / However, if you have an unresolved complaint in connection with our certification, you may contact our independent dispute resolution provider based in the \[EU/United States\], \[Dispute Resolution Provider Name\]. Please visit \[Dispute Resolution Provider URL\] for more information or to file a complaint. These services are provided to you free of charge.\]](#)

In limited situations, [\[EU\]](#), [\[UK\]](#), and [\[Swiss\]](#) individuals may seek redress from the Privacy Shield Panel, a binding arbitration mechanism.

Please be sure to review the following sections of this privacy notice for additional details relevant to our participation in the [\[EU-US\]](#) and [\[Swiss-US\]](#) Privacy Shield:

- [WHAT INFORMATION DO WE COLLECT?](#) *To learn more about the types of personal data we collect.*
- [HOW DO WE PROCESS YOUR INFORMATION?](#) *To learn more about the purposes for which we collect and use personal information about you.*

- [WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?](#) *To learn more about the type or identity of third parties to which we disclose personal information, and the purposes for which we do so.*
- [WHAT ARE YOUR PRIVACY RIGHTS?](#) *To learn more about the right of individuals to access their personal data.*

9. HOW LONG DO WE KEEP YOUR INFORMATION?

In Short: *We keep your information for as long as necessary to fulfill the purposes outlined in this privacy notice unless otherwise required by law.*

We will only keep your personal information for as long as it is necessary for the purposes set out in this privacy notice, unless a longer retention period is required or permitted by law (such as tax, accounting, or other legal requirements). No purpose in this notice will require us keeping your personal information for longer than [\[the period of time in which users have an account with us / \[#\] months past the termination of the user's account / \[#\] months past the start of the idle period of the user's account / other\]](#).

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize such information, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

10. HOW DO WE KEEP YOUR INFORMATION SAFE?

In Short: *We aim to protect your personal information through a system of organizational and technical security measures.*

We have implemented appropriate and reasonable technical and organizational security measures designed to protect the security of any personal information we process. However, despite our safeguards and efforts to secure your information, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security and improperly collect, access, steal, or modify your information. Although we will do our best to protect your personal information, transmission of personal information to and from our Services is at your own risk. You should only access the Services within a secure environment.

11. DO WE COLLECT INFORMATION FROM MINORS?

In Short: We do not knowingly collect data from or market to children under 18 years of age.

We do not knowingly solicit data from or market to children under 18 years of age. By using the Services, you represent that you are at least 18 or that you are the parent or guardian of such a minor and consent to such minor dependent's use of the Services. If we learn that personal information from users less than 18 years of age has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we may have collected from children under age 18, please contact us at [\[Email Address\]](#).

12. WHAT ARE YOUR PRIVACY RIGHTS?

In Short: In some regions, such as the European Economic Area (EEA), United Kingdom (UK), Switzerland, and Canada, you have rights that allow you greater access to and control over your personal information. You may review, change, or terminate your account at any time.

In some regions (like the EEA, UK, Switzerland, and Canada), you have certain rights under applicable data protection laws. These may include the right (i) to request access and obtain a copy of your personal information, (ii) to request rectification or erasure; (iii) to restrict the processing of your personal information; (iv) if applicable, to data portability; and (v) not to be subject to automated decision-making. In certain circumstances, you may also have the right to object to the processing of your personal information. You can make such a request by contacting us by using the contact details provided in the section "[HOW CAN YOU CONTACT US ABOUT THIS NOTICE?](#)" below.

We will consider and act upon any request in accordance with applicable data protection laws.

If you are located in the EEA or UK and you believe we are unlawfully processing your personal information, you also have the right to complain to your [Member State data protection authority](#) or [UK data protection authority](#).

If you are located in Switzerland, you may contact the [Federal Data Protection and Information Commissioner](#).

Withdrawing your consent: If we are relying on your consent to process your personal information, which may be express and/or implied consent depending on the applicable law, you have the right to withdraw your consent at any time. You can withdraw your consent at any time by contacting us by using the contact details provided in the section "[HOW CAN YOU CONTACT US ABOUT THIS NOTICE?](#)" below or updating your preferences.

However, please note that this will not affect the lawfulness of the processing before its withdrawal nor, when applicable law allows, will it affect the processing of your personal information conducted in reliance on lawful processing grounds other than consent.

Opting out of marketing and promotional communications: You can unsubscribe from our marketing and promotional communications at any time by clicking on the unsubscribe link in the emails that we send, replying “STOP” or “UNSUBSCRIBE” to the SMS messages that we send, [\[Other\]](#) or by contacting us using the details provided in the section "[HOW CAN YOU CONTACT US ABOUT THIS NOTICE?](#)" below. You will then be removed from the marketing lists – however, we may still communicate with you, for example to send you service-related messages that are necessary for the administration and use of your account, to respond to service requests, or for other non-marketing purposes.

Account Information

If you would at any time like to review or change the information in your account or terminate your account, you can:

- Log in to your account settings and update your user account.
- Contact us using the contact information provided.
- [\[Other\]](#)

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, we may retain some information in our files to prevent fraud, troubleshoot problems, assist with any investigations, enforce our legal terms and/or comply with applicable legal requirements.

Cookies and similar technologies: Most Web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and to reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features or services of our Services. You may also [opt out of interest-based advertising by advertisers](#) on our Services. For further information, please see our Cookie Notice: [\[Cookie Notice URL\]](#).

If you have questions or comments about your privacy rights, you may email us at [\[Email Address\]](#).

13. CONTROLS FOR DO-NOT-TRACK FEATURES

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your

online browsing activities monitored and collected. At this stage no uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this privacy notice.

14. DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?

In Short: *If you are a resident of California, Colorado, Connecticut, Utah, or Virginia, you are granted specific rights regarding access to your personal information.*

What categories of personal information do we collect?

We have collected the following categories of personal information in the past twelve (12) months:

Category	Examples	Collected
A. Identifiers	Contact details, such as real name, alias, postal address, telephone or mobile contact number, unique personal identifier, online identifier, Internet Protocol address, email address, and account name	[YES/NO]
B. Personal information as defined in the California Customer Records statute	Name, contact information, education, employment, employment history, and financial information	[YES/NO]
C. Protected classification characteristics under state or federal law	Gender and date of birth	[YES/NO]
D. Commercial information	Transaction information, purchase history, financial details, and payment information	[YES/NO]
E. Biometric information	Fingerprints and voiceprints	[YES/NO]

F. Internet or other similar network activity	Browsing history, search history, online behavior, interest data, and interactions with our and other websites, applications, systems, and advertisements	[YES/NO]
G. Geolocation data	Device location	[YES/NO]
H. Audio, electronic, visual, thermal, olfactory, or similar information	Images and audio, video or call recordings created in connection with our business activities	[YES/NO]
I. Professional or employment-related information	Business contact details in order to provide you our Services at a business level or job title, work history, and professional qualifications if you apply for a job with us	[YES/NO]
J. Education information	Student records and directory information	[YES/NO]
K. Inferences drawn from collected personal information	Inferences drawn from any of the collected personal information listed above to create a profile or summary about, for example, an individual's preferences and characteristics	[YES/NO]
L. Sensitive personal information	Account login information, drivers' licenses, health data, precise geolocation, racial or ethnic origin, religious or philosophical beliefs, and sex life or sexual orientation	[YES/NO]

We will use and retain the collected personal information as needed to provide the Services or for:

- Category A - [\[Retention Period\]](#)
- Category B - [\[Retention Period\]](#)
- Category C - [\[Retention Period\]](#)
- Category D - [\[Retention Period\]](#)
- Category E - [\[Retention Period\]](#)
- Category F - [\[Retention Period\]](#)

- Category G - [\[Retention Period\]](#)
- Category H - [\[Retention Period\]](#)
- Category I - [\[Retention Period\]](#)
- Category J - [\[Retention Period\]](#)
- Category K - [\[Retention Period\]](#)
- Category L - [\[Retention Period\]](#)

Category L information may be used, or disclosed to a service provider or contractor, for additional, specified purposes. You have the right to limit the use or disclosure of your sensitive personal information.

We may also collect other personal information outside of these categories through instances where you interact with us in person, online, or by phone or mail in the context of:

- Receiving help through our customer support channels;
- Participation in customer surveys or contests; and
- Facilitation in the delivery of our Services and to respond to your inquiries.

How do we use and share your personal information?

Learn about how we use your personal information in the section, "[HOW CAN YOU CONTACT US ABOUT THIS NOTICE?](#)"

We collect and share your personal information through:

- Targeting cookies/Marketing cookies
- Social media cookies
- Beacons/Pixels/Tags
- Click redirects: [\[Click Redirects\]](#)
- Social media plugins: [\[Social Media Plugins\]](#). We use social media features, such as a "Like" button, and widgets, such as a "Share" button in our Services. Such features may process your Internet Protocol (IP) address and track which page you are visiting on our website. We may place a cookie to enable the feature to work correctly. If you are logged in on a certain social media platform and you interact with a widget or button belonging to that social media platform, this information may be recorded to your profile of such social media platform. To avoid this, you should log out from that social media platform before accessing or using the Services. Social media features and widgets may be hosted by a third party or hosted directly on our Services. Your interactions with these features are governed by the privacy notices of the companies that provide them. By clicking on one of these buttons, you agree to the use of this plugin and consequently the transfer of personal information to the corresponding social media service. We

have no control over the essence and extent of these transmitted data or their additional processing.

- [\[Other\]](#)

Will your information be shared with anyone else?

We may disclose your personal information with our service providers pursuant to a written contract between us and each service provider. Learn more about who we disclose personal information to in the section, "[WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?](#)"

We may use your personal information for our own business purposes, such as for undertaking internal research for technological development and demonstration. This is not considered to be "selling" of your personal information.

We have disclosed the following categories of personal information to third parties for a business or commercial purpose in the preceding twelve (12) months:

- Category A. Identifiers
- Category B. Personal information, as defined in the California Customer Records law
- Category C. Characteristics of protected classifications under state or federal law
- Category D. Commercial information
- Category E. Biometric information
- Category F. Internet or other electronic network activity information
- Category G. Geolocation data
- Category H. Audio, electronic, visual, and similar information
- Category I. Professional or employment-related information
- Category J. Education information
- Category K. Inferences drawn from collected personal information
- Category L. Sensitive personal information

The categories of third parties to whom we disclosed personal information for a business or commercial purpose can be found under "[WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?](#)"

[We have not sold or shared any personal information to third parties for a business or commercial purpose in the preceding twelve \(12\) months. / We have sold or shared the following categories of personal information to third parties in the preceding twelve \(12\) months:](#)

- [Category A. Identifiers](#)

- Category B. Personal information, as defined in the California Customer Records law
- Category C. Characteristics of protected classifications under state or federal law
- Category D. Commercial information
- Category E. Biometric information
- Category F. Internet or other electronic network activity information
- Category G. Geolocation data
- Category H. Audio, electronic, visual, and similar information
- Category I. Professional or employment-related information
- Category J. Education information
- Category K. Inferences drawn from collected personal information
- Category L. Sensitive personal information

The categories of third parties to whom we sold personal information are:

- Ad Networks
- Affiliate Marketing Programs
- Data Analytics Services
- Retargeting Platforms
- Social Networks
- User Account Registration & Authentication Services
- [Other]

The categories of third parties to whom we shared personal information with are:

- Ad Networks
- Affiliate Marketing Programs
- Data Analytics Services
- Retargeting Platforms
- Social Networks
- User Account Registration & Authentication Services
- [Other]

California Residents

California Civil Code Section 1798.83, also known as the "Shine The Light" law, permits our users who are California residents to request and obtain from us, once a year and free of charge, information about categories of personal information (if any) we disclosed to third parties for direct marketing purposes and the names and addresses of all third parties with which we shared personal information in the

immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to us using the contact information provided below.

If you are under 18 years of age, reside in California, and have a registered account with Services, you have the right to request removal of unwanted data that you publicly post on the Services. To request removal of such data, please contact us using the contact information provided below and include the email address associated with your account and a statement that you reside in California. We will make sure the data is not publicly displayed on the Services, but please be aware that the data may not be completely or comprehensively removed from all our systems (e.g., backups, etc.).

CCPA Privacy Notice

This section applies only to California residents. Under the California Consumer Privacy Act (CCPA), you have the rights listed below.

The California Code of Regulations defines a "resident" as:

- (1) every individual who is in the State of California for other than a temporary or transitory purpose and
- (2) every individual who is domiciled in the State of California who is outside the State of California for a temporary or transitory purpose

All other individuals are defined as "non-residents."

If this definition of "resident" applies to you, we must adhere to certain rights and obligations regarding your personal information.

Your rights with respect to your personal data

Right to request deletion of the data – Request to delete

You can ask for the deletion of your personal information. If you ask us to delete your personal information, we will respect your request and delete your personal information, subject to certain exceptions provided by law, such as (but not limited to) the exercise by another consumer of his or her right to free speech, our compliance requirements resulting from a legal ob`

Depending on the circumstances, you have a right to know:

- whether we collect and use your personal information;

- the categories of personal information that we collect;
- the purposes for which the collected personal information is used;
- whether we sell or share your personal information to third parties;
- the categories of personal information that we sold, shared, or disclosed for a business purpose;
- the categories of third parties to whom the personal information was sold, shared, or disclosed for a business purpose;
- the business or commercial purpose for collecting, sharing, or selling personal information; and
- the specific pieces of personal information we collected about you.

In accordance with applicable law, we are not obligated to provide or delete consumer information that is de-identified in response to a consumer request or to re-identify individual data to verify a consumer request.

Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights

We will not discriminate against you if you exercise your privacy rights.

Right to Limit Use and Disclosure of Sensitive Personal Information

[We do not process consumer's sensitive personal information. / If the business collects any of the following:

- social security information, drivers' licenses, state ID cards, passport numbers
- account login information
- credit card numbers, financial account information, or credentials allowing access to such accounts
- precise geolocation
- racial or ethnic origin, religious or philosophical beliefs, union membership
- the contents of email and text, unless the business is the intended recipient of the communication
- genetic data, biometric data, and health data
- data concerning sexual orientation and sex life

you have the right to direct that business to limit its use of your sensitive personal information to that use which is necessary to perform the Services.

Once a business receives your request, they are no longer allowed to use or disclose your sensitive personal information for any other purpose unless you provide consent for the use or disclosure of sensitive personal information for additional purposes.

Please note that sensitive personal Information that is collected or processed without the purpose of inferring characteristics about a consumer is not covered by this right, as well as the publicly available information.

To exercise your right to limit use and disclosure of sensitive personal Information, please email [Email Address] or visit: [DSAR Form URL].

Verification process

Upon receiving your request, we will need to verify your identity to determine you are the same person about whom we have the information in our system. These verification efforts require us to ask you to provide information so that we can match it with information you have previously provided us. For instance, depending on the type of request you submit, we may ask you to provide certain information so that we can match the information you provide with the information we already have on file, or we may contact you through a communication method (e.g., phone or email) that you have previously provided to us. We may also use other verification methods as the circumstances dictate.

We will only use personal information provided in your request to verify your identity or authority to make the request. To the extent possible, we will avoid requesting additional information from you for the purposes of verification. However, if we cannot verify your identity from the information already maintained by us, we may request that you provide additional information for the purposes of verifying your identity and for security or fraud-prevention purposes. We will delete such additionally provided information as soon as we finish verifying you.

Other privacy rights

- You may object to the processing of your personal information.
- You may request correction of your personal data if it is incorrect or no longer relevant, or ask to restrict the processing of the information.
- You can designate an authorized agent to make a request under the CCPA on your behalf. We may deny a request from an authorized agent that does not submit proof that they have been validly authorized to act on your behalf in accordance with the CCPA.
- [You may request to opt out from future selling or sharing of your personal information to third parties. Upon receiving an opt-out request, we will act upon the request as soon as feasibly possible, but no later than fifteen (15) days from the date of the request submission.]

[You can opt out from the selling or sharing of your personal information by disabling cookies in Cookie Preference Settings and clicking on the Do Not Sell or Share My Personal Information link on our homepage.]

To exercise these rights, you can contact us by visiting [\[DSAR Form URL\]](#), by email at [\[Email Address\]](#), by calling toll-free at [\[Phone Number\]](#), by visiting [\[Contact Form URL\]](#), or by referring to the contact details at the bottom of this document. If you have a complaint about how we handle your data, we would like to hear from you.

Financial Incentives

"Financial incentive" means a program, benefit, or other offering, including payments to consumers as compensation, for the disclosure, deletion, sharing, or sale of personal information.

The law permits financial incentives or a price or service difference if it is reasonably related to the value of the consumer's data. A business must be able to explain how the financial incentive or price or service difference is reasonably related to the value of the consumer's data. The explanation must include:

- a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and
- a description of the method the business used to calculate the value of the consumer's data.

We may decide to offer a financial incentive (e.g., price or service difference) in exchange for the retention, or sale or sharing of a consumer's personal information.

If we decide to offer a financial incentive, we will notify you of such financial incentive and explain the price difference, as well as material terms of the financial incentive or price of service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference.

If you choose to participate in the financial incentive you can withdraw from the financial incentive at any time by emailing us at [\[Email Address\]](#), by calling us toll-free at [\[Phone Number\]](#), by visiting [\[Contact Form URL\]](#), or by referring to the contact details at the bottom of this document.

Metrics

Our metrics for all CCPA requests received for the previous calendar year can be found here: [\[Metrics URL\]](#).

Colorado Residents

This section applies only to Colorado residents. Under the Colorado Privacy Act (CPA), you have the rights listed below. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by law.

- Right to be informed whether or not we are processing your personal data
- Right to access your personal data
- Right to correct inaccuracies in your personal data
- Right to request deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to opt out of the processing of your personal data if it is used for targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects (“profiling”)

[\[We sell personal data to third parties or process personal data for targeted advertising. You can opt out from the selling of your personal data, targeted advertising, or profiling by disabling cookies in Cookie Preference Settings.\]](#) To submit a request to exercise these rights described above, please email [\[Email Address\]](#) or visit [\[DSAR Form URL\]](#).

If we decline to take action regarding your request and you wish to appeal our decision, please email us at [\[Email Address\]](#). Within forty-five (45) days of receipt of an appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions.

Connecticut Residents

This section applies only to Connecticut residents. Under the Connecticut Data Privacy Act (CTDPA), you have the rights listed below. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by law.

- Right to be informed whether or not we are processing your personal data
- Right to access your personal data
- Right to correct inaccuracies in your personal data
- Right to request deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to opt out of the processing of your personal data if it is used for targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects (“profiling”)

[\[We sell personal data to third parties or process personal data for targeted advertising. You can opt out from the selling of your personal data, targeted advertising, or profiling by disabling cookies in Cookie](#)

[Preference Settings.](#) To submit a request to exercise these rights described above, please email [\[Email Address\]](#) or visit [\[DSAR Form URL\]](#).

If we decline to take action regarding your request and you wish to appeal our decision, please email us at [\[Email Address\]](#). Within sixty (60) days of receipt of an appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions.

Utah Residents

This section applies only to Utah residents. Under the Utah Consumer Privacy Act (UCPA), you have the rights listed below. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by law.

- Right to be informed whether or not we are processing your personal data
- Right to access your personal data
- Right to request deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to opt out of the processing of your personal data if it is used for targeted advertising or the sale of personal data

[\[We sell personal data to third parties or process personal data for targeted advertising. You can opt out from the selling of your personal data, targeted advertising, or profiling by disabling cookies in Cookie Preference Settings.\]](#) To submit a request to exercise these rights described above, please email [\[Email Address\]](#) or visit [\[DSAR Form URL\]](#).

Virginia Residents

Under the Virginia Consumer Data Protection Act (VCDPA):

"Consumer" means a natural person who is a resident of the Commonwealth acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.

"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include de-identified data or publicly available information.

"Sale of personal data" means the exchange of personal data for monetary consideration.

If this definition of "consumer" applies to you, we must adhere to certain rights and obligations regarding your personal data.

Your rights with respect to your personal data

- Right to be informed whether or not we are processing your personal data
- Right to access your personal data
- Right to correct inaccuracies in your personal data
- Right to request deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to opt out of the processing of your personal data if it is used for targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects ("profiling")

[We sell personal data to third parties or process personal data for targeted advertising. Please see the following section to find out how you can opt out from further selling or sharing of your personal data for targeted advertising or profiling purposes.]

Exercise your rights provided under the Virginia VCDPA

[You can opt out from the selling of your personal data, targeted advertising, or profiling by disabling cookies in Cookie Preference Settings.]

You may contact us by email at [Email Address] or visit [Contact Form URL].

If you are using an authorized agent to exercise your rights, we may deny a request if the authorized agent does not submit proof that they have been validly authorized to act on your behalf.

Verification process

We may request that you provide additional information reasonably necessary to verify you and your consumer's request. If you submit the request through an authorized agent, we may need to collect additional information to verify your identity before processing your request.

Upon receiving your request, we will respond without undue delay, but in all cases, within forty-five (45) days of receipt. The response period may be extended once by forty-five (45) additional days when reasonably necessary. We will inform you of any such extension within the initial 45-day response period, together with the reason for the extension.

Right to appeal

If we decline to take action regarding your request, we will inform you of our decision and reasoning behind it. If you wish to appeal our decision, please email us at [\[Email Address\]](#). Within sixty (60) days of receipt of an appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If your appeal is denied, you may contact the [Attorney General to submit a complaint](#).

15. DO OTHER REGIONS HAVE SPECIFIC PRIVACY RIGHTS?

In Short: *You may have additional rights based on the country you reside in.*

Australia and New Zealand

We collect and process your personal information under the obligations and conditions set by Australia's Privacy Act 1988 and New Zealand's Privacy Act 2020 (Privacy Act).

This privacy notice satisfies the notice requirements defined in both Privacy Acts, in particular: what personal information we collect from you, from which sources, for which purposes, and other recipients of your personal information.

If you do not wish to provide the personal information necessary to fulfill their applicable purpose, it may affect our ability to provide our services, in particular:

- offer you the products or services that you want
- manage your account with us
- respond to or help with your requests
- confirm your identity and protect your account

At any time, you have the right to request access to or correction of your personal information. You can make such a request by contacting us by using the contact details provided in the section "[HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?](#)"

If you believe we are unlawfully processing your personal information, you have the right to submit a complaint about a breach of the Australian Privacy Principles to the [Office of the Australian Information Commissioner](#) and for a breach of New Zealand's Privacy Principles to the [Office of New Zealand Privacy Commissioner](#).

Republic of South Africa

At any time, you have the right to request access to or correction of your personal information. You can make such a request by contacting us by using the contact details provided in the section "[HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?](#)"

If you are unsatisfied with the manner in which we address any complaint with regard to our processing of personal information, you can contact the office of the regulator, the details of which are:

[The Information Regulator \(South Africa\)](#)

General enquiries: enquiries@inforegulator.org.za

Complaints (complete POPIA/PAIA form 5): PAIAComplaints@inforegulator.org.za & POPIAComplaints@inforegulator.org.za

16. DO WE MAKE UPDATES TO THIS NOTICE?

In Short: Yes, we will update this notice as necessary to stay compliant with relevant laws.

We may update this privacy notice from time to time. The updated version will be indicated by an updated "Revised" date and the updated version will be effective as soon as it is accessible. If we make material changes to this privacy notice, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this privacy notice frequently to be informed of how we are protecting your information.

17. HOW CAN YOU CONTACT US ABOUT THIS NOTICE?

If you have questions or comments about this notice, you may contact our Data Protection Officer (DPO), [\[DPO Name\]](#), by email at [\[Email Address\]](#), by phone at [\[Phone Number\]](#), or by post to:

[\[Company Name\]](#)

[\[DPO Name\]](#)

[\[Street Address\]](#)

[\[City, State ZIP Code\]](#)

[\[Country\]](#)

If you are a resident in the European Economic Area or Switzerland, we are the "data controller" of your personal information. We have appointed [\[EEA Representative Name\]](#) to be our representative in the EEA and Switzerland. You can contact them directly regarding our processing of your information, by email at [\[Email Address\]](#), by visiting [\[EEA Representative URL\]](#), by phone at [\[Phone Number\]](#), or by post to:

[Street Address]

[City, State ZIP Code]

[Country]

Swiss Representative

[Swiss Representative Name]

[Street Address]

[City, State ZIP Code]

[Country]

Phone: [Phone Number]

Fax: [Fax Number]

[Swiss Representative URL]

If you are a resident in the United Kingdom, we are the "data controller" of your personal information. We have appointed [UK Representative Name] to be our representative in the UK. You can contact them directly regarding our processing of your information, by email at [Email Address], by visiting [UK Representative URL], by phone at [Phone Number], or by post to:

[Street Address]

[City, State ZIP Code]

[Country]

If you have any further questions or comments, you may also contact us by post at the following corporate address:

[Company Name]

[Street Address]

[City, State ZIP Code]

[Country]

Phone: [Phone Number]

Fax: [Fax Number]

18. HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?

Based on the applicable laws of your country, you may have the right to request access to the personal information we collect from you, change that information, or delete it. To request to review, update, or delete your personal information, please visit: [DSAR Form URL].

PRIVACY POLICY FOR CALIFORNIA RESIDENTS

Effective date: 03/08/2021

This Privacy Policy applies to any California residents about whom we have collected personal information from any source, including through your use of our Sites, by buying products or services, or by communicating with us electronically, in paper correspondence, or in person (collectively, “you”). We provide this to comply with applicable privacy laws, including the California Consumer Privacy Act of 2018 (“CCPA”) and the California Privacy Rights Act of 2020 (“CPRA”). Any capitalized term used and not otherwise defined below has the meaning assigned to it in the online Privacy Policy.

The CCPA and CPRA provides California residents with rights to receive certain disclosures regarding the collection, use, and sharing of “personal information,” as well as rights to access, delete, and restrict the sale of certain personal information we collect about them. California residents also have the right not to receive discriminatory treatment by us for the exercise of your privacy rights under the CCPA and CPRA. If you are a California resident, you may submit a request to exercise these rights by completing the online webform or by emailing us at privacy@beatstars.com. For more information about our general privacy practices, please view our online .

If you are a visually-impaired customer, a customer who has another disability or a customer who seek support in other language, you may access BeatStars’ Privacy Policy for California Residents by emailing .

I. DEFINITIONS

For the purposes of this Privacy Policy, except where a different definition is noted, “personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California consumer/resident or household. Personal information does not include publicly available information, information that has been de-identified or aggregated, or other information covered by certain sector-specific privacy laws.

II. CCPA DISCLOSURES AND RIGHTS

A. Personal Information We Collect

BeatStars may collect, or has collected, the following categories of personal information about you over the last twelve (12) months:

Identifiers, which includes your name and username; birthday; email address, mailing address, and telephone number; online identifiers as detailed below including IP address or device IDs; name, and password; government-issued identification card number; and/or other similar identifiers.

Payment and financial information, including your credit or debit card number, PayPal email address, and/or other financial information.

Commercial information, which includes records of music recordings; products or services including subscriptions purchased, obtained, or considered; participation in working with Sony Music Publishing; account balances, payment history, or account activity; bank account information and other information relating to your financial institution; and/or other purchasing or consumer histories or tendencies.

Information relating to Internet activity or other electronic network activity, which includes your browsing history and Site usage information, interactions with ads, IP address, cookie identifiers, clear gifs (web beacons/web bugs), browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp, device platform, and device version.

Geolocation data, which includes Global Positioning System (“GPS”) data based on your IP address.

Audio, electronic, or visual information, which includes music recordings, images and comment that you or others submit to our Site to be featured, displayed, or streamed on our Site; and recordings of calls to or from our customer service centers.

Inferences drawn from personal information listed above which includes preferences, such as your listening preferences, interests and other information, used create a profile about you in order for us to personalize ads and content.

Information not listed above and related to characteristics protected under California or federal law, which may include gender, if you display it on your profile or elsewhere on the platform.

B. What We Do With Your Information

BeatStars may collect, use, or disclosure personal information about you for the following purposes:

Provide our Services to you (such as account registration) and maintain the Platform and your account;

Market and sell our products and services;

Bill you for services and process subscription payments;

Provide you with a personalized content and ads;

Operate and maintain safe, secure and reliable Services and Sites;

Improve our operational efficiency and provide you with better products and services;

Perform research and development;

Contact you in response to an inquiry that you sent;

Send you messages and information related to our products and services, support and administrative messages, technical notices, updates, alerts, and other information;

Send you information about services and programs we offer that may be of interest to you;

Recommend artists to our business partners for publishing engagements;

Detect and prevent fraud and abuse, including perform identity verification;

Perform accounting, audits and other internal functions; and

Comply with request or order from courts, law enforcement or other government authorities.

BeatStars may also use personal information for other business purposes, including the following: (i) perform accounting, audits and other internal functions; (ii) compliance with our legal obligations or to assert or defend a legal claim; (iii) general business administration; (iii) processing employment applications; and (iv) systems and data security.

C. Sources of Collected Information

We may collect personal information from the following categories of sources:

From you, including via our Sites, telephone, postal mail, social media, forums, or other means

Business partnersthat promote and/or offer services

Advertising networks

Social networkswith whom you choose to connect your BeatStars account to

Other third parties, which includes payment portals you opt to use outside of those authorized by us,

operators of other websites and mobile applications, and other data suppliers

Other sources, including things that other third parties may post publicly about you or otherwise provide to us

We may supplement the information described above with information we obtain from other sources, including from both online and offline data providers.

D. Who We Share Your Information With

We limit our disclosure of the categories of personal information above to our service providers for one or more business purposes. We may also provide your personal identifiers such as name, email address, and phone number to our business partners, but not limited to including Sony Music Publishing, for consideration for potential publishing when you have expressly directed us to do so by filling out a publishing application.

We do not sell your personal information to third parties, including personal information of minors under 16 years of age. As with nearly every e-commerce company, we do share a limited set of data that is gathered when you visit our Site, such as cookies and pixels, with third parties in order to allow you to see tailored digital advertisements. To the extent this activity is interpreted as included in California's broad definition of "data sale", we have provided you with opt-out rights as to that activity as described in Section II(f) below.

In the last twelve (12) months, we've disclosed certain personal information to the following categories of third parties:

Categories of third parties	Categories of personal information disclosed
-----------------------------	--

Other users and artists through the Services, including artists	
---	--

Identifiers; audio, electronic, or visual information; and information related to characteristics protected under California or federal law	
---	--

Business partners such as Sony Music Publishing	
---	--

Identifiers; commercial information; and audio, electronic, or visual information	
---	--

Advertising partners	
----------------------	--

Identifiers; information relating to Internet activity or other electronic network activity; geolocation data; inferences drawn	
---	--

Social networks	
-----------------	--

Identifiers; information relating to Internet activity or other electronic network activity; audio, electronic, or visual information; information related to characteristics protected under California or federal law	
---	--

If you are a minor under the age of 18 residing in the State of California, United States, You have additional rights under California law. You may request removal of any information or content you posted while under the age of 18. We cannot ensure that removal of information you provided to the Service will be complete or comprehensive (i.e., information posted to public groups and forums that may be accessed by non-users) but it will be complete and comprehensive on our part (i.e., user account information).

E. Data Protection

This Data Protection section applies to all users of any services owned or controlled by Beatstars Inc. Furthermore, this section extends to Service Providers, Contractors, Affiliates, Vendors, Affiliates, Agents, and Entities; their parent company and subsidiaries, or their respective employees, officers, directors, members, managers, shareholders, agents, vendors, licensors, licensees, contractors, customers, successors, and assigns (each referred to as "Parties" in the following paragraph). By executing any Agreement with Beatstars Inc., which uses any personal information, Parties agree to abide by the following paragraph. Violation of this section is cause for termination of Service or rights granted by Beatstars, Inc. Moreover, if an agreement has been executed between Beatstars Inc. and a Party, violation of this section is considered a material breach.

Each party shall, at its own expense, ensure that it complies with and assists Beatstars Inc. to comply with the requirements of all legislation and regulatory requirements in force from time to time relating to the use of personal data, including (without limitation) (i) any U.S. Data Protection legislation, including but not limited to the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). This clause is in addition to, and does not reduce, remove or replace, a party's obligations arising from such requirements hereunder. You confirm that you will not rent or sell customer lists, contact details or other data without the customers' express prior approval.

F. Your Privacy Rights

If you are a California resident, you have the following rights under applicable California law in relation to your personal information, subject to certain exceptions:

Right to Know. You have the right to, up to twice in a 12-month period, request what personal information we collect, use, disclose, and/or sell, as applicable.

Right to Delete. You have the right to request under certain circumstances the deletion of your personal information that is collected by us.

Right to Opt-Out of Sale or Sharing. You have the right to opt-out of the sale or sharing of your personal information by a business.

Right to Non-Discrimination. You have the right not to receive discriminatory treatment for the exercise of the privacy rights described above.

Right to Correct. You have the right to correct your information to exercise your privacy rights described above.

Any request you submit to us is subject to an identification and residency verification process ("Verifiable Consumer Request") as permitted by the CCPA. We will not fulfill your request unless you have provided sufficient information that enables us to reasonably verify that you are the consumer about whom we collected the personal information on. In order to verify you, you must provide us with your email address and your BeatStars username. These rights are also subject to various exclusions and exceptions under applicable laws.

You may also designate an authorized agent, in writing or through a power of attorney, to request to exercise the above rights on your behalf. The authorized agent may submit a request to exercise these rights by emailing the letter of authorization or power of attorney to .

We currently do not collect household data. If we receive a Right to Know or Right to Delete request submitted by all members of a household, we will individually respond to each request. We will not be able to comply with any request by a member of a household under the age of 13, as we do not collect personal information from any person under the age of 13.

We will respond to your request within forty-five (45) days after receipt of a Verifiable Consumer Request for a period covering twelve (12) months and for no more than twice in a twelve-month period. BeatStars reserves the right to extend the response time by an additional forty-five (45) days when reasonably necessary and provided consumer notification of the extension is made within the first forty-five (45) days.

You may exercise any of the rights described in this section by completing the online webform or by emailing us at .

G. Notice of Right to Opt-Out

We do not sell your personal information. If you wish to opt-out of our sharing of the limited data that is gathered when you visit our Site for purposes of targeted digital advertising, we encourage you to visit the and/or the Digital Advertising Alliance's for more information about opting out of seeing targeted digital advertisements. You may also visit these websites for more information on how you can opt back in to the sharing of data. Please note that BeatStars does not maintain this web tracking data in an identifiable manner. California-based users can opt out of performance, targeting, and social media cookies and SDKs by selecting the "Do Not Sell or Share My Personal Information" link in their cookie or SDK settings.

You can use these resources or other plugins to opt out of cookies through your browser:

Common browser settings:

We will continue to update our business practices as direct regulatory guidance becomes available. For more information on interest-based advertising, please visit our and .

H. How To Contact Us

If you have any questions about this Privacy Policy or our privacy practices, please contact us by completing the online webform or by emailing us at .

I. CALIFORNIA "SHINE THE LIGHT" LAW

California residents additionally have the right to request information regarding third parties to whom BeatStars has disclosed certain categories of personal information during the preceding year for the third parties' direct marketing purposes under California's "Shine the Light" law (Cal. Civ. Code §1798.83). Personal information under this California law means "any information that when it was disclosed identified, described, or was able to be associated with an individual." We do not disclose this type of personal information to third parties for their own purposes and we permit you to opt-out of any disclosures of non-identifiable personal information. However, if you are a California resident and would like to inquire further, please email .

Do not sell my personal information

Effective date: 06/06/2022

BeatStars Inc. ("BeatStars", "us", "we", or "our") is 100% committed to our customers and community, which is why we want to take the time to explain exactly what the "Do Not Sell My Personal Information" link on BeatStars webpages and apps means. The purpose of this article is to explain (1) why BeatStars' webpages and apps contain the "Do Not Sell" link, (2) what it means to "sell" "personal information," as those terms are defined under California law (3) that BeatStars does not sell personal information that directly identifies you, even under the California definition of "sale," (4) what happens if you tell BeatStars not to "sell" your personal information, (5) how BeatStars implements your choice to block it from "selling" your personal information, and (6) how BeatStars maintains your "Do Not Sell" Choice.

Why Does BeatStars Provide the "Do Not Sell" Link?

BeatStars provides the "Do Not Sell" link to comply with the California Consumer Privacy Act (CCPA), California Civil Code Section 1798.100 et seq., effective January 1, 2020. The CCPA is a new data protection law that provides California residents with certain choices about their data, including the ability to tell companies not to "sell" their personal information. The link is there to inform you of this choice. Although the CCPA only gives California residents the right to make these requests, we allow non-California residents with the same choices about their personal information. Please see our for more information.

What Does it Mean to "Sell" "Personal Information" Under the CCPA?

The CCPA broadens the definition of "sale" and "personal information" beyond how you might commonly interpret those terms.

Under the CCPA, "personal information" includes information that is not necessarily directly tied to an individual's identity but may be associated with a device. This includes identifiers such as IP addresses, web cookies, web beacons, and mobile AdIDs. In many cases, this type of information is not associated with you, but they are unique identifiers that could be. Similarly, the term "sell" is defined to include not just selling in exchange for money, but also sharing or transferring personal information (including information that does not directly identify an individual as described above) in exchange for anything of value, which is not limited to the exchange of money. Certain things are not considered "sales," including when (1) personal information is shared with a service provider that is contractually prohibited from using the personal information for any purpose beyond the service specifically requested ("service provider exception"), or (2) when the consumer has directed a company to disclose the personal information ("consumer directed exception").

Does BeatStars "Sell" my Personal Information?

BeatStars does not sell information that directly identifies you, like your name, address, social security number, banking information, or phone records. In fact, we do not even share that type of information except

with service providers who can use the information solely to provide a service on our behalf, when a consumer directs us to share the information, or in the limited additional circumstances outlined in our (such as for fraud prevention purposes or where we are legally required to share the information).

However, the CCPA's broad definitions of "sale" and "personal information" may deem the common flow of information in the digital analytics and advertising ecosystem to be a sale. Like most companies that operate commercial websites and apps, BeatStars utilizes online analytics to measure the ways users engage with our websites and apps. These analytics, in turn, inform how we perform online advertising. In order to provide these analytics and facilitate online advertising, BeatStars uses third-parties that collect device identifiers and place tags, cookies, beacons, and similar tracking mechanisms on our websites/apps and on third-party websites/apps. For instance, we may request that a third-party facilitate the placement of BeatStars ads on a particular website after a consumer has previously visited BeatStars. The third-parties we use for these purposes generally do this by placing a cookie on a user's browser so it can identify that the same browser visited other websites. Similarly, where our webpages or apps provide space for advertisements, these third-parties may use identifiers such as cookies for websites, or the device's mobile AdID for apps, to facilitate real-time bidding by advertisers.

Where we can reasonably ensure via contract that the third-parties described above can and will use a device identifier solely to provide the specific service we have requested, and will not use or share the data for other purposes, we will not deem that sharing a "sale." In most cases, we've determined that our data analytics providers that measure the ways users engage with our websites and apps meet this standard and, accordingly, we will not block the sharing of an identifier with those entities even when you choose to opt-out through the "Do Not Sell" link.

In some cases, though, BeatStars does not ultimately control how such identifiers are used by some third-parties (particularly in some cases in the online advertising ecosystem), and so we can't determine that all sharing with third-parties in these cases fall within the service provider exception under the law.

What Happens when I Tell BeatStars not to "Sell" my Personal Information?

When a user of our websites/apps makes the "Do Not Sell" choice, we will attempt to block further sharing of the covered identifiers with the third-parties we engage on those digital properties or any other entity that does not fall within the service provider exception or the consumer directed exception.

How Does BeatStars Implement my Choice to Block it from "Selling" my Personal Information?

If you wish to opt-out of our sharing of the limited data that is gathered when you visit our Site for purposes of targeted digital advertising, we encourage you to visit the , the or the for more information about opting out of seeing targeted digital advertisements. Similarly, you can learn about your options to opt-out of mobile app tracking by certain advertising networks through your device settings.

You may also visit these websites for more information on how you can opt back into the sharing of data.

You can also opt out of interest-based advertising with some of the service providers we use, such as Google .

If you would like to exercise any of these rights, please contact us by emailing us at .

How Does BeatStars Maintain my "Do Not Sell" Choice?

If you choose to sign in and set a "Do Not Sell" setting tied to your account, we will attempt to identify and honor that setting on the BeatStars app or website. Please note that that setting may not work if your browser does not accept cookies or if you later delete cookies or delete data on your app.

Ad choices settings and options will vary depending on your browser and device settings, and this is not an exhaustive list. Please note that your opt-out choices will only apply to the specific browser or device from which you opt out. Please explore your device and browser settings to better understand your choices.

Connected devices (such as tablets, connected TVs, and other devices) may also use an advertising ID or other methods to identify you or serve you interest-based advertising. In some cases, you can disable tracking by selecting options like “limit ad tracking” or disabling options like “interest-based advertising” in your connected device’s settings. These options will vary by device and we do not control the policies or practices of third parties’ providing these devices. BeatStars is not responsible for tracking on connected devices or our business partners’ services and may not have visibility on choices you may have made with respect to tracking on connected devices or our business partners’ services.

For information on how to control your choices on those devices, you should contact those third parties directly to learn more about their privacy practices and any data they may collect and share or sell to third parties.

For more information about BeatStars’ privacy practices and our approach to the CCPA, please see our .

GDPR Privacy Notice

Effective date: 28/07/2022

The purpose of the General Data Protection Regulation ("GDPR") is to protect all European Union ("EU") citizens from privacy and data breaches by allowing citizens to maintain control of the personal data kept and processed by organizations, which includes BeatStars Inc ("BeatStars", "us", "we", or "our") . The GDPR also protects the personal data of individuals, regardless of citizenry, in the EU.

BeatStars is committed to safeguarding the privacy of personal data. Furthermore, BeatStars is committed to protecting your privacy online. We are also committed to providing you with the very best experience we can on our website at BeatStars.com and BeatStars mobile (our “Sites”) and all related sites and other web-based services that enable website visitor access on our behalf, including players, widgets, tools and other services provided by BeatStars (collectively, the "Services"). This Policy also describes how we use personal data, the purpose for sharing and recipients of personal data and your rights and choices associated with that data. By using BeatStars, you are consenting to the practices described in this Privacy Notice.

Use of Information

Our primary goal in collecting personal information is to provide you, the user, with a customized experience on our website. We use the collected data for various purposes including:

- To provide and maintain our Sites and Services, including to take steps to enter into a contract for sale or services, bill you for services and process payments and fulfill transactions;
- To enable and allow you to participate in interactive features of our Sites and Services and provide you with a personalized service, content and ads;
- To create custom audiences on social media sites;
- To provide you with better products and services and improve and grow our business, including to perform research and development, understand our customer base and purchasing trends and understand the effectiveness of our marketing;
- To operate and maintain safe, secure and reliable Sites and Services;
- To provide customer support, including to contact you in response to an inquiry that you sent, and send administrative messages, technical notices, updates, alerts and other information;
- To provide you with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless you have opted not to receive such information;
- To track the progress and number of entries in our promotions and contests;
- To contact you on behalf of certain artists or other third parties and recommend artists to our business partners for publishing engagements;
- To perform accounting, audits and other internal functions; and
- To comply with a request or order from courts, law enforcement or other government authorities.

BeatStars may also use personal information for other business purposes, including the following: (i) perform accounting, audits and other internal functions; (ii) compliance with our legal obligations or to assert or defend a legal claim; (iii) general business administration; (iii) processing employment applications; and (iv) systems and data security.

In addition, if we feel that a user abuses the BeatStars.com site in any way, we reserve the right to use and share certain information with third parties. Abuses include (but are not limited to) possible copyright infringement, possible libel and slander, and possible fraudulent or illegal activity.

Third Party Use of Sensitive Information

We may disclose your Sensitive Information and other Information as follows:

Consent: We may disclose Information if we have your consent to do so.

Emergency Circumstances: We may share your Information when necessary to protect your interests and you are physically or legally incapable of providing consent.

Employment Necessity: We may share your Information when necessary for administering employment or social security benefits in accordance with applicable law or any applicable collective bargaining agreement, subject to the imposition of appropriate safeguards to prevent further unauthorized disclosure.

Public Information: We may share your Information if you have manifestly made it public.

Archiving: We may share your Information for archival purposes in the public interest, and for historical research and statistical purposes.

Performance of a Contract: We may share your Information when necessary to administer a contract you have with the BeatStars.

Legal Obligation: We may share your Information when the disclosure is required or permitted by international, federal, and state laws and regulations.

Service Providers: We use third parties who have entered into a contract with the BeatStars. In such cases, we share your Information with such third parties subject to the imposition of appropriate safeguards to prevent further unauthorized disclosure.

BeatStars Affiliates: We may share your Information with parties that are affiliated with the BeatStars for the purpose of contacting you about goods, services, charitable giving or experiences that may be of interest to you.

De-Identified and Aggregate Information: We may use and disclose Information in de-identified or aggregate form without limitation.

Security

We implement appropriate technical and organizational security measures to protect your information when you transmit it to us and when we store it on our information technology systems.

Cookies and Other Technology

The BeatStars use of cookies and other data can be found in the BeatStars' Privacy Policy.

Retention and Destruction of Your Information

Your information will be retained by the BeatStars in accordance with applicable state and federal laws, and the applicable retention periods in the Privacy Policy. Your information will be destroyed upon your request unless applicable law requires destruction after the expiration of an applicable retention period. The manner of destruction shall be appropriate to preserve and ensure the confidentiality of your information given the level of sensitivity, value and criticality to the BeatStars.

Your Rights

You have the right to request access to, a copy of, rectification, restriction in the use of, or erasure of your information in accordance with all applicable laws. The erasure of your information shall be subject to applicable state and federal laws, and the applicable retention periods in the BeatStars Privacy Policy. If you have provided consent to the use of your information, you have the right to withdraw consent without affecting the lawfulness of the BeatStars' use of the information prior to receipt of your request.

Information created in the European Union will be transferred out of the European Union to the BeatStars. If you feel BeatStars has not complied with applicable foreign laws regulating such information, you have the right to file a complaint with the appropriate supervisory authority in the European Union.

Updates to This Policy

We may update or change this policy at any time. Your continued use of the BeatStars' website and third party applications after any such change indicates your acceptance of these changes.

Contact Us

If you have any questions about this GDPR Policy or wish to exercise one of your Data Subject rights, please contact us:

By emailing us: ;

By visiting [page](#) on our website.

Privacy policy

Effective: January 31, 2024

We've updated our Privacy Policy below. These updates do not apply to individuals located in the European Economic Area, UK, and Switzerland. If you reside in those areas, this version of our Privacy Policy applies to you.

We at OpenAI OpCo, LLC (together with our affiliates, "OpenAI", "we", "our" or "us") respect your privacy and are strongly committed to keeping secure any information we obtain from you or about you. This Privacy Policy describes our practices with respect to Personal Information we collect from or about you when you use our website, applications, and services (collectively, "Services"). This Privacy Policy does not apply to content that we process on behalf of customers of our business offerings, such as our API. Our use of that data is governed by our customer agreements covering access to and use of those offerings.

For information about how we collect and use training information to develop our language models that power ChatGPT and other Services, and your choices with respect to that information, please see this [help center article](#)(opens in a new window).

1. Personal information we collect

We collect personal information relating to you ("Personal Information") as follows:

Personal information you provide: We collect Personal Information if you create an account to use our Services or communicate with us as follows:

Account Information: When you create an account with us, we will collect information associated with your account, including your name, contact information, account credentials, payment card information, and transaction history, (collectively, "Account Information").

User Content: When you use our Services, we collect Personal Information that is included in the input, file uploads, or feedback that you provide to our Services ("Content").

Communication Information: If you communicate with us, we collect your name, contact information, and the contents of any messages you send ("Communication Information").

Social Media Information: We have pages on social media sites like Instagram, Facebook, Medium, Twitter, YouTube and LinkedIn. When you interact with our social media pages, we will collect Personal Information

that you elect to provide to us, such as your contact details (collectively, “Social Information”). In addition, the companies that host our social media pages may provide us with aggregate information and analytics about our social media activity.

Other Information You Provide: We collect other information that you may provide to us, such as when you participate in our events or surveys or provide us with information to establish your identity (collectively, “Other Information You Provide”)

Personal information we receive automatically from your use of the Services: When you visit, use, or interact with the Services, we receive the following information about your visit, use, or interactions (“Technical Information”):

Log Data: Information that your browser or device automatically sends when you use our Services. Log data includes your Internet Protocol address, browser type and settings, the date and time of your request, and how you interact with our Services.

Usage Data: We may automatically collect information about your use of the Services, such as the types of content that you view or engage with, the features you use and the actions you take, as well as your time zone, country, the dates and times of access, user agent and version, type of computer or mobile device, and your computer connection.

Device Information: Includes name of the device, operating system, device identifiers, and browser you are using. Information collected may depend on the type of device you use and its settings.

Cookies: We use cookies to operate and administer our Services, and improve your experience. A “cookie” is a piece of information sent to your browser by a website you visit. You can set your browser to accept all cookies, to reject all cookies, or to notify you whenever a cookie is offered so that you can decide each time whether to accept it. However, refusing a cookie may in some cases preclude you from using, or negatively affect the display or function of, a website or certain areas or features of a website. For more details on cookies, please visit [All About Cookies](#)(opens in a new window).

Analytics: We may use a variety of online analytics products that use cookies to help us analyze how users use our Services and enhance your experience when you use the Services.

2. How we use personal information

We may use Personal Information for the following purposes:

To provide, administer, maintain and/or analyze the Services;

To improve our Services and conduct research;

To communicate with you; including to send you information about our Services and events;

To develop new programs and services;

To prevent fraud, criminal activity, or misuses of our Services, and to protect the security of our IT systems, architecture, and networks;

To carry out business transfers; and

To comply with legal obligations and legal process and to protect our rights, privacy, safety, or property, and/or that of our affiliates, you, or other third parties.

Aggregated or de-identified information. We may aggregate or de-identify Personal Information so that it may no longer be used to identify you and use such information to analyze the effectiveness of our Services, to improve and add features to our Services, to conduct research and for other similar purposes. In addition, from time to time, we may analyze the general behavior and characteristics of users of our Services and share aggregated information like general user statistics with third parties, publish such aggregated information or make such aggregated information generally available. We may collect aggregated information through the Services, through cookies, and through other means described in this Privacy Policy. We will maintain and use de-identified information in anonymous or de-identified form and we will not attempt to reidentify the information, unless required by law.

As noted above, we may use Content you provide us to improve our Services, for example to train the models that power ChatGPT. Read our instructions([opens in a new window](#)) on how you can opt out of our use of your Content to train our models.

3. Disclosure of personal information

In certain circumstances we may provide your Personal Information to third parties without further notice to you, unless required by the law:

Vendors and Service Providers: To assist us in meeting business operations needs and to perform certain services and functions, we may provide Personal Information to vendors and service providers, including providers of hosting services, customer service vendors, cloud services, email communication software, web analytics services, and other information technology providers, among others. Pursuant to our instructions, these parties will access, process, or store Personal Information only in the course of performing their duties to us.

Business Transfers: If we are involved in strategic transactions, reorganization, bankruptcy, receivership, or transition of service to another provider (collectively, a “Transaction”), your Personal Information and other information may be disclosed in the diligence process with counterparties and others assisting with the Transaction and transferred to a successor or affiliate as part of that Transaction along with other assets.

Legal Requirements: We may share your Personal Information, including information about your interaction with our Services, with government authorities, industry peers, or other third parties (i) if required to do so by law or in the good faith belief that such action is necessary to comply with a legal obligation, (ii) to protect and defend our rights or property, (iii) if we determine, in our sole discretion, that there is a violation of our terms, policies, or the law; (iv) to detect or prevent fraud or other illegal activity; (v) to protect the safety, security, and integrity of our products, employees, or users, or the public, or (vi) to protect against legal liability.

Affiliates: We may disclose Personal Information to our affiliates, meaning an entity that controls, is controlled by, or is under common control with OpenAI. Our affiliates may use the Personal Information we share in a manner consistent with this Privacy Policy.

Business Account Administrators: When you join a ChatGPT Enterprise or business account, the administrators of that account may access and control your OpenAI account. In addition, if you create an account using an email address belonging to your employer or another organization, we may share the fact that you have an OpenAI account and certain account information, such as your email address, with your employer or organization to, for example, enable you to be added to their business account.

Other Users and Third Parties You Share Information With: Certain features allow you to display or share information with other users or third parties. For example, you may share ChatGPT conversations with other users via shared links or send information to third-party applications via custom actions for GPTs. Be sure you trust any user or third party with whom you share information.

4. Your rights

Depending on location, individuals may have certain statutory rights in relation to their Personal Information. For example, you may have the right to:

Access your Personal Information and information relating to how it is processed.

Delete your Personal Information from our records.

Rectify or update your Personal Information.

Transfer your Personal Information to a third party (right to data portability).

Restrict how we process your Personal Information.

Withdraw your consent—where we rely on consent as the legal basis for processing at any time.

Object to how we process your Personal Information.

Lodge a complaint with your local data protection authority.

You can exercise some of these rights through your OpenAI account. If you are unable to exercise your rights through your account, please submit your request through privacy.openai.com (opens in a new window) or to dsar@openai.com.

A note about accuracy: Services like ChatGPT generate responses by reading a user's request and, in response, predicting the words most likely to appear next. In some cases, the words most likely to appear next may not be the most factually accurate. For this reason, you should not rely on the factual accuracy of output from our models. If you notice that ChatGPT output contains factually inaccurate information about you and you would like us to correct the inaccuracy, you may submit a correction request through privacy.openai.com (opens in a new window) or to dsar@openai.com. Given the technical complexity of how our models work, we may not be able to correct the inaccuracy in every instance. In that case, you may request that we remove your Personal Information from ChatGPT's output by filling out this form (opens in a new window).

For information on how to exercise your rights with respect to data we have collected from the internet to train our models, please see this help center article (opens in a new window).

5. Additional U.S. state disclosures

The following table provides additional information about the categories of Personal Information we collect and how we disclose that information. You can read more about the Personal Information we collect in "Personal information we collect" above, how we use Personal Information in "How we use personal information" above, and how we retain Personal Information in "Security and Retention" below.

Category of Personal Information

Disclosure of Personal Information

Identifiers, such as your name, contact details, IP address, and other device identifiers

We may disclose this information to our affiliates, vendors and service providers to process in accordance with our instructions; to law enforcement and other third parties for the legal reasons described above; to parties involved in Transactions; to corporate administrators of enterprise or team accounts; and to other users and third parties you choose to share it with.

Commercial Information, such as your transaction history

We may disclose this information to our affiliates, vendors and service providers to process in accordance with our instructions; to law enforcement and other third parties for the legal reasons described above; to parties involved in Transactions; and to corporate administrators of enterprise or team accounts.

Network Activity Information, such as Content and how you interact with our Services

We may disclose this information to our affiliates, vendors and service providers to process in accordance with our instructions; to law enforcement and other third parties for the legal reasons described above; to parties involved in Transactions; and to other users and third parties you choose to share it with.

Geolocation Data

We may disclose this information to our affiliates, vendors and service providers to process in accordance with our instructions; to law enforcement and other third parties for the legal reasons described above; and to parties involved in Transactions.

Your account login credentials and payment card information (Sensitive Personal Information)

We disclose this information to our affiliates, vendors and service providers, law enforcement, and parties involved in Transactions.

To the extent provided for by local law and subject to applicable exceptions, individuals may have the following privacy rights in relation to their Personal Information:

The right to know information about our processing of your Personal Information, including the specific pieces of Personal Information that we have collected from you;

The right to request deletion of your Personal Information;

The right to correct your Personal Information; and

The right to be free from discrimination relating to the exercise of any of your privacy rights.

We don't "sell" Personal Information or "share" Personal Information for cross-contextual behavioral advertising (as those terms are defined under applicable local law). We also don't process sensitive Personal Information for the purposes of inferring characteristics about a consumer.

Exercising your rights. To the extent applicable under local law, you can exercise privacy rights described in this section by submitting a request through privacy.openai.com (opens in a new window) or to dsar@openai.com.

Verification. In order to protect your Personal Information from unauthorized access, change, or deletion, we may require you to verify your credentials before you can submit a request to know, correct, or delete Personal Information. If you do not have an account with us, or if we suspect fraudulent or malicious activity, we may ask you to provide additional Personal Information and proof of residency for verification. If we cannot verify your identity, we will not be able to honor your request.

Authorized agents. You may also submit a rights request through an authorized agent. If you do so, the agent must present signed written permission to act on your behalf and you may also be required to independently verify your identity and submit proof of your residency with us. Authorized agent requests can be submitted to dsar@openai.com.

Appeals. Depending on where you live, you may have the right to appeal a decision we make relating to requests to exercise your rights under applicable local law. To appeal a decision, please send your request to dsar@openai.com.

6. Children

Our Service is not directed to children under the age of 13. OpenAI does not knowingly collect Personal Information from children under the age of 13. If you have reason to believe that a child under the age of 13 has provided Personal Information to OpenAI through the Service, please email us at legal@openai.com. We will investigate any notification and if appropriate, delete the Personal Information from our systems. If you are 13 or older, but under 18, you must have permission from your parent or guardian to use our Services.

7. Links to other websites

The Service may contain links to other websites not operated or controlled by OpenAI, including social media services ("Third Party Sites"). The information that you share with Third Party Sites will be governed by the specific privacy policies and terms of service of the Third Party Sites and not by this Privacy Policy. By providing these links we do not imply that we endorse or have reviewed these sites. Please contact the Third Party Sites directly for information on their privacy practices and policies.

8. Security and retention

We implement commercially reasonable technical, administrative, and organizational measures to protect Personal Information both online and offline from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. However, no Internet or email transmission is ever fully secure or error free. In particular, email sent to or from us may not be secure. Therefore, you should take special care in deciding what information you send to us via the Service or email. In addition, we are not responsible for circumvention of any privacy settings or security measures contained on the Service, or third-party websites.

We'll retain your Personal Information for only as long as we need in order to provide our Service to you, or for other legitimate business purposes such as resolving disputes, safety and security reasons, or complying with our legal obligations. How long we retain Personal Information will depend on a number of factors, such as the amount, nature, and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure, our purpose for processing the information, and any legal requirements.

9. International users

By using our Service, you understand and acknowledge that your Personal Information will be processed and stored in our facilities and servers in the United States and may be disclosed to our service providers and affiliates in other jurisdictions.

Legal basis for processing. Our legal bases for processing your Personal Information include:

Performance of a contract with you when we provide and maintain our Services. When we process Account Information, Content, and Technical Information solely to provide our Services to you, this information is necessary to be able to provide our Services. If you do not provide this information, we may not be able to provide our Services to you.

Our legitimate interests in protecting our Services from abuse, fraud, or security risks, or in developing, improving, or promoting our Services, including when we train our models. This may include the processing of Account Information, Content, Social Information, and Technical Information. Read our instructions([opens in a new window](#)) on how you can opt out of our use of your information to train our models.

Your consent when we ask for your consent to process your Personal Information for a specific purpose that we communicate to you. You have the right to withdraw your consent at any time.

Compliance with our legal obligations when we use your Personal Information to comply with applicable law or when we protect our or our affiliates', users', or third parties' rights, safety, and property.

Data transfers. Where required, we will use appropriate safeguards for transferring Personal Information outside of certain countries. We will only transfer Personal Information pursuant to a legally valid transfer mechanism.

Data protection officer. You can contact our data protection officer at privacy@openai.com in matters related to Personal Information processing.

10. Changes to the privacy policy

We may update this Privacy Policy from time to time. When we do, we will post an updated version on this page, unless another type of notice is required by applicable law.

11. How to contact us

Please contact [support](#) (opens in a new window) if you have any questions or concerns not already addressed in this Privacy Policy.

Privacy Policy

Last Updated: [Date]

1. Introduction

Welcome to [Your Company Name] (“Company”, “we”, “our”, “us”). We are committed to protecting your personal data and your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you visit our website [Website URL], and your rights in relation to that information.

2. Information We Collect

We may collect and process the following data about you:

- *Personal Identification Information*: Name, email address, phone number, etc.
- *Technical Data*: IP address, browser type, operating system, referring URLs, access times, and pages viewed.
- *Usage Data*: Information on how you use our website, products, and services.
- *Marketing and Communications Data*: Your preferences in receiving marketing from us and your communication preferences.
- *Financial Data*: Payment card details, transaction details.

3. How We Collect Information

We collect information in the following ways:

- *Direct Interactions*: You may provide data by filling in forms on our site, subscribing to our services, or communicating with us by post, phone, email, or otherwise.
- *Automated Technologies or Interactions*: As you interact with our site, we may automatically collect Technical Data about your equipment, browsing actions, and patterns.

- ***Third Parties or Publicly Available Sources***: We may receive personal data about you from various third parties and public sources.

4. How We Use Your Information

We use the information we collect for the following purposes:

- To provide, operate, and maintain our website and services.
- To improve, personalize, and expand our website and services.
- To understand and analyze how you use our website and services.
- To develop new products, services, features, and functionality.
- To communicate with you, either directly or through one of our partners, including for customer service, to provide you with updates and other information relating to the website, and for marketing and promotional purposes.
- To process your transactions and manage your orders.
- To comply with legal obligations and to enforce our terms, conditions, and policies.

5. Legal Basis for Processing Personal Data (GDPR)

If you are from the European Economic Area (EEA), [Company Name]'s legal basis for collecting and using the personal information described in this Privacy Policy depends on the Personal Data we collect and the specific context in which we collect it. We may process your Personal Data because:

- We need to perform a contract with you.
- You have given us permission to do so.
- The processing is in our legitimate interests and it is not overridden by your rights.
- To comply with the law.

6. Your Rights (GDPR)

If you are a resident of the EEA, you have the following data protection rights:

- The right to access, update, or to delete the information we have on you.
- The right of rectification.
- The right to object.
- The right of restriction.
- The right to data portability.
- The right to withdraw consent.

7. Your Rights (CCPA/CPRA)

If you are a California resident, you have the following rights:

- The right to know what personal information is being collected about you.
- The right to access personal information.
- The right to know whether your personal information is sold or disclosed and to whom.

- The right to say no

Certainly! Below is a comprehensive privacy policy template designed to comply with GDPR, CCPA, CPRA, and other relevant privacy laws. Please customize this template to suit your specific business needs.

Privacy Policy

Last Updated: [Date]

1. Introduction

Welcome to [Your Company Name] ("Company", "we", "our", "us"). We are committed to protecting your personal data and your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you visit our website [Website URL], and your rights in relation to that information.

2. Information We Collect

We may collect and process the following types of personal data:

- *Personal Identification Information*: Name, email address, phone number, postal address, and other similar contact data.
- *Technical Data*: IP address, browser type, operating system, device identifiers, referring URLs, access times, and pages viewed.
- *Usage Data*: Information about how you use our website, products, and services.
- *Marketing and Communications Data*: Your preferences in receiving marketing from us and your communication preferences.
- *Financial Data*: Payment card details, billing address, and transaction history.

3. How We Collect Information

We collect information through:

- *Direct Interactions*: You provide personal data when you fill in forms, subscribe to our services, request information, or communicate with us.
- *Automated Technologies*: As you interact with our site, we may automatically collect Technical Data using cookies, server logs, and other similar technologies.
- *Third Parties*: We may receive personal data from third-party services, partners, and publicly available sources.

4. Use of Your Information

We use the collected data for various purposes, including:

- ***Provision of Services***: To provide, operate, and maintain our website and services.
- ***Improvement***: To improve, personalize, and expand our website and services.
- ***Analysis***: To understand and analyze how you use our website and services.
- ***Development***: To develop new products, services, features, and functionality.
- ***Communication***: To communicate with you, including for customer service, updates, and marketing purposes.
- ***Transactions***: To process your transactions and manage your orders.
- ***Legal Compliance***: To comply with legal obligations and to enforce our terms and conditions.

5. Legal Basis for Processing Personal Data (GDPR)

For individuals in the European Economic Area (EEA), our legal basis for processing your personal data includes:

- ***Contractual Necessity***: To perform a contract with you.
- ***Consent***: Where you have given us consent.
- ***Legitimate Interests***: For our legitimate interests, provided your rights do not override these interests.
- ***Legal Obligations***: To comply with applicable laws.

6. Your Rights (GDPR)

If you are an EEA resident, you have the following rights regarding your personal data:

- ***Access***: The right to request access to your personal data.
- ***Rectification***: The right to request correction of inaccurate data.
- ***Erasure***: The right to request deletion of your data.
- ***Restriction***: The right to request restriction of processing.
- ***Data Portability***: The right to request transfer of your data.
- ***Objection***: The right to object to processing.
- ***Withdraw Consent***: The right to withdraw consent at any time.

7. Your Rights (CCPA/CPRA)

If you are a California resident, you have the following rights under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA):

- ***Right to Know***: The right to know what personal information is collected about you.
- ***Right to Access***: The right to access your personal information.
- ***Right to Delete***: The right to request deletion of your personal information.
- ***Right to Opt-Out***: The right to opt-out of the sale of your personal information.
- ***Right to Non-Discrimination***: The right to not be discriminated against for exercising your privacy rights.

8. Data Security

We implement appropriate technical and organizational measures to protect your personal data from unauthorized access, use, or disclosure.

9. Data Retention

We retain your personal data only as long as necessary

please contact us at:

- *Email*: [Your Contact Email]
- *Postal Address*: [Your Company Address]
- *Phone Number*: [Your Contact Number]

14. Your Choices

- *Marketing Communications*: You can opt-out of receiving marketing emails from us at any time by following the unsubscribe link in the email or by contacting us directly.
- *Cookies*: Most web browsers are set to accept cookies by default. You can usually choose to set your browser to remove or reject cookies. If you choose to remove or reject cookies, this could affect certain features or services of our website.

15. Third-Party Links

Our website may contain links to third-party websites. We are not responsible for the privacy practices or the content of those websites. We encourage you to review the privacy policies of any third-party websites you visit.

16. Your Privacy Rights Under Other Jurisdictions

Depending on your jurisdiction, you may have additional privacy rights. We are committed to upholding all applicable data protection laws. Please contact us if you have any questions about your privacy rights.

17. Data Protection Officer

If you are a resident of the European Economic Area (EEA) or the United Kingdom (UK), you can contact our Data Protection Officer at [DPO Contact Information] for any data protection inquiries.

18. Governing Law

This Privacy Policy is governed by the laws of [Your Jurisdiction], without regard to its conflict of law principles.

19. Complaints

If you believe your privacy rights have been violated, you have the right to lodge a complaint with the relevant supervisory authority in your jurisdiction.

Appendix: Definitions

- *Personal Data*: Any information relating to an identified or identifiable natural person.
- *Processing*: Any operation or set of operations performed on personal data.
- *Controller*: The natural or legal

Certainly! Here is the continuation of the privacy policy:

Appendix: Definitions (Continued)

- *Consent*: Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them.
- *Legitimate Interests*: Interests that are considered valid legal grounds for processing personal data, provided that the processing is not overridden by the data subject's rights and interests.

20. Additional Information for Residents of Specific Jurisdictions

Australia

- *Access and Correction*: You have the right to request access to your personal information and to request its correction if it is inaccurate, out-of-date, incomplete, irrelevant, or misleading. To make such a request, please contact us using the details provided in the "Contact Us" section.
- *Complaints*: If you believe we have breached the Australian Privacy Principles, you can contact us to lodge a complaint. We will respond to your complaint within a reasonable time.

Canada

- *Access and Correction*: You have the right to access and correct your personal information held by us. You may request access to your personal data or seek to correct it by contacting us using the details provided in the "Contact Us" section.
- *Complaints*: If you have any concerns about our privacy practices, you may contact the Office of the Privacy Commissioner of Canada.

Brazil

- ***Access and Correction***: You have the right to request access to, correction of, and deletion of your personal data. You may also request information about the processing of your personal data.

- ***Data Protection Officer***: Our Data Protection Officer for Brazil can be contacted using the details provided in the "Contact Us" section.

- ***Complaints***: If you have any concerns about our privacy practices, you may contact the National Data Protection Authority (ANPD).

21. Data Subject Requests

We are committed to responding to your requests to exercise your privacy rights in a timely manner. To make a request, please contact us using the details provided in the "Contact Us" section. We may need to verify your identity before processing your request.

- ***Verification Process***: To verify your identity, we may request information that matches the personal data we have on file for you. This is to ensure that your data is protected and only accessed by you or your authorized representative.

22. Authorized Agents

You may designate an authorized agent to make a request on your behalf. To designate an authorized agent, you must provide written permission and verify your own identity with us. Authorized agents may also need to provide proof of their authority to act on your behalf.

23. Do Not Track

Our website does not respond to Do Not Track (DNT) signals. However, we adhere to the privacy standards outlined in this Privacy Policy, regardless of DNT signals.

24. Changes to This Privacy Policy

We reserve the right to update this Privacy Policy at any time. When we make changes, we will revise the "Last Updated" date at the top of this page. We encourage you to review this Privacy Policy periodically to stay informed about how we are protecting your information.

25. Effective Date

This Privacy Policy is effective as

Certainly! Here's the final part of the privacy policy template, including more comprehensive information for other jurisdictions and any additional details you might want to include.

27. Additional Information for Residents of Specific Jurisdictions (Continued)

United Kingdom

- ***Access and Correction***: Under the UK General Data Protection Regulation (UK GDPR), you have the right to request access to your personal data and to request its correction if it is inaccurate or incomplete. To exercise these rights, please contact us using the details provided in the "Contact Us" section.

- ***Complaints***: If you have concerns about how we are handling your personal data, you have the right to lodge a complaint with the Information Commissioner's Office (ICO).

China

- ***Access and Correction***: You have the right to request access to and correction of your personal data. To make such a request, please contact us using the details provided in the "Contact Us" section.

- ***Complaints***: If you believe we have not complied

Certainly! Here is the completed section on cookies, along with a template for a detailed Cookie Policy:

Absolutely, a comprehensive privacy policy should cover a wide range of topics to ensure transparency and compliance with relevant privacy laws. Here are the key points typically included:

1. ***Introduction***: Provide an overview of your commitment to privacy and the purpose of the policy.

2. ***Types of Information Collected***: Detail the categories of personal information collected, including identifiers, demographic information, commercial information, internet or other electronic network activity, geolocation data, etc.

3. ***Sources of Information***: Specify how you collect personal information, such as directly from users, through automated means (cookies, web beacons), or from third parties.

4. ***Purposes of Data Collection***: Explain the purposes for which you collect and process personal information, including providing services, improving user experience, marketing, and advertising.

5. ***Legal Basis for Processing***: Outline the legal grounds for processing personal data, such as consent, contractual necessity, legitimate interests, compliance with legal obligations, etc.

6. ***Data Sharing***: Describe how and with whom you share personal information, including third-party service providers, affiliates, business partners, or in response to legal requests.

7. ***Data Retention***: Specify how long you retain personal information and the criteria used to determine retention periods.

8. ***User Rights***: Inform users of their rights regarding their personal data, including the right to access, rectify, erase, restrict processing, object to processing, and data portability.

9. ***Data Security Measures***: Explain the security measures implemented to protect personal information from unauthorized access, disclosure, alteration, or destruction.

10. ***International Data Transfers***: If applicable, disclose if personal data is transferred internationally and the safeguards in place to protect data when transferred outside the originating country.

12. ***Children's Privacy***: State whether your services are directed to children under 13 or 16 years old, depending on applicable regulations, and

Certainly! Continuing from where we left off:

19. ***Third-party Services***: Disclose any third-party services or applications integrated into your website or services, and clarify how they handle personal data, including any data shared with them.

20. ***Data Subject Requests***: Explain how users can exercise their privacy rights, such as accessing, correcting, or deleting their personal information, and provide instructions on how to submit such requests.

21. ***Authorized Agents***: If applicable, explain how users can designate authorized agents to exercise their privacy rights on their behalf and the verification process for such requests.

22. ***Automated Decision Making***: Disclose if you engage in automated decision-making processes, including profiling, and provide information about the logic involved and the potential consequences for users.

23. ***Data Breach Notification***: Outline procedures for notifying users and authorities in the event of a data breach, including the timing and content of notifications.

24. ***User Consent***: Explain how user consent is obtained for processing personal data, including cookie consent mechanisms and options for withdrawing consent.

25. ***Opt-out Mechanisms***: Provide users with options to opt-out of certain data processing activities, such as marketing communications or targeted advertising.

26. ***Data Controller and Processor Information***: Specify the roles and responsibilities of data controllers and processors, including contact information

Of course! Here are some more points to consider for a comprehensive privacy policy:

34. ***User Education***: Provide educational resources or links to resources that help users understand privacy rights, data protection, and best practices for safeguarding personal information.
35. ***Cross-border Data Transfers***: If you transfer personal data across borders, explain how you ensure the protection of data during such transfers, including reliance on standard contractual clauses, binding corporate rules, or other legal mechanisms.
36. ***Record-keeping***: Establish procedures for maintaining records of data processing activities, including purposes of processing, categories of personal data, recipients of data, and retention periods.
37. ***Privacy by Design***: Incorporate privacy considerations into the design and development of products and services from the outset, following principles of privacy by design and default.
38. ***Data Impact Assessments***: Conduct data protection impact assessments (DPIAs) for high-risk processing activities to identify and mitigate privacy risks to individuals.
39. ***Training and Awareness***: Implement training programs to ensure that employees understand their responsibilities regarding data protection and privacy compliance.
40. ***Vendor Management***: Establish contractual agreements with third-party vendors and service providers to ensure they comply with applicable data protection laws and maintain adequate security measures.
41. ***User Authentication and Access Controls***: Implement user authentication mechanisms and access controls to prevent unauthorized access to personal data and ensure data security.
42. ***Data Portability***: Enable users to request and receive their personal data in a structured, commonly used, and machine-readable format, and provide mechanisms for transferring data to other services.
43. ***Incident Response Plan***: Develop and maintain an incident response plan to address data breaches or other security incidents promptly and effectively.
44. ***Privacy Notices***: Provide supplemental privacy notices or disclosures at the point of data collection, such as on web forms or mobile apps, to inform users about specific data processing activities.
45. ***Data Minimization***: Limit the collection and processing of personal data to what is necessary for the intended purpose and avoid unnecessary or excessive data collection.
46. ***Whistleblower Policy***: Establish procedures for employees to report privacy violations or concerns internally, ensuring confidentiality and protection against retaliation.
47. ***Data Governance Framework***: Implement a data governance framework to manage and control the lifecycle of personal data, including data quality, integrity, and accountability.

48. ***Independent Audits***: Conduct regular independent audits or assessments of your privacy practices to verify compliance with applicable laws and regulations.

49. ***Consumer Education***: Educate consumers about their privacy rights, responsibilities, and options for protecting their personal information through informational materials or online resources.

50. ***Public Accountability***: Demonstrate commitment to privacy protection and accountability through public statements, transparency reports, or participation in privacy certification programs.

By incorporating these additional points into your privacy policy and privacy management practices, you can enhance transparency, accountability, and trust with your users while promoting compliance with relevant privacy laws and regulations.

Certainly! Here are more points to consider for a comprehensive privacy policy:

51. ***User Consent Mechanisms***: Describe how users can provide consent to the collection, processing, and sharing of their personal data, including the use of checkboxes, opt-in/opt-out forms, or other consent mechanisms.

52. ***Sensitive Data***: Specify if you collect or process sensitive personal data (e.g., health information, racial or ethnic origin, political opinions) and the additional protections in place for such data.

53. ***Data Subject Rights Procedures***: Detail the procedures and timelines for responding to data subject rights requests, including verification of identity and communication methods.

54. ****Data**

Apologies for the oversight. Let's continue with more comprehensive points for a privacy policy:

70. ***Data Localization***: Specify if personal data is stored or processed in specific jurisdictions and any legal requirements or agreements related to data localization.

71. ***Geolocation Data***: If you collect geolocation data, explain the purposes for which it's used, how it's collected (e.g., GPS, IP address), and users' options for controlling geolocation tracking.

72. ***Data Anonymization and Pseudonymization***: Describe techniques used to anonymize or pseudonymize personal data to protect user privacy and confidentiality.

73. ***Profiling for Marketing and Advertising***: If user profiling is used for targeted marketing or advertising purposes, disclose the types of data used, how profiles are created, and users' rights to opt-out.

74. ***User Consent Logs***: Maintain records of user consent, including timestamps, the scope of consent, and how consent was obtained, to demonstrate compliance with consent requirements.

75. ***Data Processing Agreements***: Enter into data processing agreements with third parties that process personal data on your behalf, outlining their obligations and responsibilities regarding data protection.

76. ***Security Incident Notification Requirements***: Describe any legal or regulatory requirements related to notifying users, authorities, or other stakeholders in the event of a security incident or data breach.

77. ***Data Subject Access Requests (DSARs)***: Explain the process for handling data subject access requests, including the timeframe for responding, verifying the requester's identity, and providing requested information.

78. ***Data Subject Rectification Requests***: Outline procedures for correcting inaccurate or incomplete personal data upon request from data subjects, including how rectifications are communicated to third parties, if applicable.

79. ***Data Subject Erasure Requests (Right to be Forgotten)***: Detail the process for honoring data subjects' requests to delete their personal data, including any exceptions or limitations under applicable law.

80. ***Data Subject Objection Requests***: Explain how data subjects can object to certain processing activities (e.g., direct marketing) and the steps taken to address objections, including ceasing processing or providing opt-out mechanisms.

81. ***Automated Decision-Making Transparency***: Provide transparency regarding automated decision-making processes, including the criteria used, the potential impact on individuals, and mechanisms for human intervention or review.

82. ***Data Subject Consent Withdrawal***: Inform users of their right to withdraw consent to processing activities and the implications of withdrawing consent, such as limitations on service availability or features.

83. ***Data Subject Complaint Escalation Procedures***: Specify escalation procedures for handling unresolved data subject complaints, including contact information for relevant supervisory authorities or dispute resolution mechanisms.

84. ***Corporate Mergers and Acquisitions***: Describe how changes in corporate ownership or structure may affect data processing activities and users' rights, including notification procedures and any impact on data protection measures.

85. ***Data Subject Rights Training for Staff***: Provide training to staff members responsible for handling data subject requests to ensure they understand their obligations and responsibilities under applicable privacy laws.

86. ***Data Subject Consent Revocation Mechanisms***: Implement mechanisms for data subjects to easily revoke consent to processing activities, such as through user account settings or dedicated opt-out mechanisms.

87. ***Data Subject Consent Documentation***: Maintain documentation of user consent, including the version of the privacy policy at the time of consent, the purpose of processing, and any specific consent preferences expressed by the user.

88. ***Data Subject Consent Confirmation***: Provide confirmation to data subjects upon the successful submission of consent preferences, including a summary of the processing activities covered by the consent and the effective date of consent.

89. ***Data Subject Consent Renewal Notices***: Periodically remind data subjects of their consent preferences and provide opportunities to review and update their consent settings, especially in cases where consent expiration dates are specified.

90. ***Data Subject Consent Withdrawal Confirmation***: Confirm the successful withdrawal of consent to data subjects and provide guidance on any additional steps they may need to take to ensure the cessation of processing activities covered by the revoked consent.

91. ***Data Subject Consent Granularity***: Offer granular consent options to data subjects, allowing them to choose specific processing activities or categories of personal data they consent to, rather than providing blanket consent.

92. ***Data Subject Consent Preferences Dashboard***: Provide data subjects with access to a consent preferences dashboard or control panel where they can manage their consent settings, view consent history, and exercise consent-related rights.

93. ***Data Subject Consent Recipients***: Disclose the recipients or categories of recipients with whom data subjects' consented personal data may be shared, along with the purposes for which the data will be shared.

94. ***Data Subject Consent Duration***: Specify the duration of data subjects' consent preferences, including any expiration dates or conditions under which consent may be automatically renewed or revoked.

95. ***Data Subject Consent Verification***: Implement mechanisms to verify data subjects' consent preferences, such as confirmation emails, two-factor authentication, or captcha tests, to prevent unauthorized changes to consent settings.

96. ***Data Subject Consent Preferences History***: Maintain a historical record of data subjects' consent preferences, including the date and time of consent changes, the specific preferences selected, and the version of the privacy policy at the time of consent.

97. ***Data Subject Consent Transparency***: Provide transparency regarding the scope and implications of data subjects' consent preferences, including explanations of processing activities covered by the consent and any associated risks or benefits.

98. ***Data Subject Consent Acknowledgment***: Require data subjects to acknowledge their understanding of the implications of providing or withholding consent to processing activities, such as through checkbox acknowledgments or digital signatures.

99. ***Data Subject Consent Revalidation***: Prompt data subjects to revalidate their consent preferences periodically

Updates to this Policy

We may update this Cookies Policy from time to time to reflect changes in our practices or for other operational, legal, or regulatory reasons. We encourage you to review this policy periodically for any updates.

Contact Us

PRIVACY POLICY

[5:14 pm, 16/05/2024] Jaled: ---

Privacy Policy

[Your Company Name] ("we," "us," or "our") is committed to protecting the privacy and security of your personal information. This Privacy Policy describes how we collect, use, and disclose personal information when you visit our website [Your Website URL] (the "Site") or interact with us through other channels. By using the Site or providing us with your personal information, you consent to the practices described in this policy.

1. Information We Collect

a. ***Personal Information***: We may collect personal information such as your name, email address, postal address, phone number, and other contact details when you voluntarily provide it to us, such as when you fill out a contact form, subscribe to our newsletter, or make a purchase.

b. ***Usage Data***: We automatically collect certain information about your device and how you interact with the Site, including your IP address, browser type, pages visited, and referring URL.

c. ***Cookies and Similar Technologies***: We use cookies and similar tracking technologies to analyze website traffic, personalize content, and provide targeted advertising. You can control cookies through your browser settings or opt-out of certain tracking technologies.

2. How We Use Your Information

We may use your personal information for the following purposes:

- To respond to your inquiries or requests.
- To process transactions and fulfill orders.
- To send you newsletters, marketing communications, or other updates.
- To analyze website usage and improve our Site's performance.
- To comply with legal obligations or enforce our terms of use.

3. Information Sharing and Disclosure

We may share your personal information with third-party service providers who assist us in operating our Site, conducting our business, or serving our users. We may also disclose your information when required by law or to protect our rights, property, or safety.

4. Data Security

We take reasonable measures to protect your personal information from unauthorized access, disclosure, alteration, or destruction. However, no method of transmission over the internet or electronic storage is 100% secure, so we cannot guarantee absolute security.

5. Your Rights and Choices

You have the right to access, update, or delete your personal information. You may also opt-out of receiving marketing communications from us by following the unsubscribe instructions included in our emails.

6. Children's Privacy

Our Site is not intended for children under the age of

[5:15 pm, 16/05/2024] Jaled: Certainly, continuing from where we left off:

6. Children's Privacy

Our Site is not intended for children under the age of 13. We do not knowingly collect personal information from children under 13. If you are a parent or guardian and believe that your child has provided us with personal information, please contact us so that we can delete the information.

7. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices or for other operational, legal, or regulatory reasons. We encourage you to review this policy periodically for any updates.

8. Contact Us

If you have any questions or concerns about this Privacy Policy, or if you would like to exercise your rights regarding your personal i...

[5:16 pm, 16/05/2024] Jaled: While the privacy policy provided covers many essential aspects, the completeness of your privacy policy depends on various factors such as the nature of your website or business, the types of personal information you collect, and applicable legal requirements in your jurisdiction.

Here are some additional considerations you may want to include in your privacy policy:

1. ***Third-party Links***: If your website contains links to third-party websites or services, you may want to include a disclaimer stating that your privacy policy does not apply to those third-party sites and that users should review the privacy policies of those sites.

2. ***International Data Transfers***: If you operate in multiple jurisdictions or transfer personal information across international borders, you may need to include information about how you comply with data protection laws governing cross-border data transfers.

3. ***Data Retention***: Specify how long you retain personal information and the criteria used to determine the retention period.

4. ***Data Subject Rights***: Inform users of their rights regarding their personal information, such as the right to access, rectify, or delete their data, and provide instructions on how to exercise those rights.

5. ***Legal Basis for Processing***: Explain the legal basis for processing personal information, such as consent, contractual necessity, legitimate interests, or compliance with legal obligations.

6. ***California Consumer Privacy Act (CCPA)***: If you collect personal information from California residents, you may need to include additional disclosures required by the CCPA, such as categories of personal information collected and rights afforded to California consumers.

7. ***European Union General Data Protection Regulation (GDPR)***: If you collect personal data from individuals in the European Economic Area (EEA), you must comply with GDPR requirements, including specific disclosures about data processing activities and data subject rights.

8. ***Data Breach Notification***: Outline your procedures for responding to data breaches, including notifying affected individuals and relevant authorities as required by

[5:16 pm, 16/05/2024] Jaled: The components provided cover many essential aspects of a privacy policy, but the completeness of your privacy policy depends on various factors such as the nature of your website or business, the types of personal information you collect, and applicable legal requirements in your jurisdiction.

To ensure your privacy policy is comprehensive and compliant, consider the following:

1. ***Legal Compliance***: Ensure your privacy policy complies with relevant laws and regulations, such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and other data protection laws applicable to your jurisdiction.

2. ***Data Collection Practices***: Clearly outline what types of personal information you collect from users and how you collect it. This includes information collected directly from users, as well as information collected automatically through cookies and similar technologies.

3. ***Purpose of Data Processing***: Explain the purposes for which you collect, use, and process personal information. This may include providing and improving your services, communicating with users, and marketing activities.

4. ***Data Sharing and Disclosure***: Disclose how you share or disclose personal information to third parties, including service providers, business partners, and other parties as required by law or with user consent.

5. ***Data Retention***: Specify how long you retain personal information and the criteria used to determine the retention period. This includes information on when and how personal data is deleted or anonymized.

6. ***User Rights***: Inform users of their rights regarding their personal information, such as the right to access, rectify, or delete their data, and provide instructions on how to exercise those rights.

7. ***Security Measures***: Describe the security measures you have in place to protect personal information. Of course, here are some bullet points for a privacy policy:

28. Cookies and Similar Technologies

We use cookies and similar tracking technologies to collect and use personal data about you, including to serve interest-based advertising. This section provides information about the types of cookies we use, their purpose, and how you can manage your cookie preferences.

Types of Cookies We Use

- ***Essential Cookies***: These

11. ***Cookies and Tracking Technologies***: Provide information about the use of cookies, web beacons, tracking pixels, and similar technologies, including the types of cookies used, their purpose, and how users can manage cookie preferences.

cookies

Cookies Policy

This Cookies Policy explains how our website uses cookies and similar tracking technologies. By accessing or using our website, you consent to the use of cookies as described in this policy.

What are Cookies?

Cookies are small text files that are placed on your computer or mobile device when you visit a website. They are widely used to make websites work more efficiently and to provide information to the owners of the site.

Types of Cookies We Use

- ***Essential Cookies***: These cookies are necessary for the website to function properly. They enable core functionalities such as security, network management, and accessibility.

- ***Analytical Cookies***: These cookies allow us to analyze how visitors use our website, so we can measure and improve its performance. We use Google Analytics and similar tools to collect information about website traffic and usage patterns.

- ***Functionality Cookies***: These cookies enable enhanced functionality and personalization, such as remembering your preferences or settings.

- ***Advertising Cookies***: These cookies are used to deliver advertisements that are relevant to you and your interests. They may be used by third-party advertisers to track your browsing activity across different websites.

Third-Party Cookies

We may also use third-party cookies provided by trusted partners for analytics, advertising, and other purposes. These cookies are subject to the respective privacy policies of the third-party providers.

Managing Cookies

You can control and/or delete cookies as you wish. Most web browsers allow you to manage cookies through their settings. You can also opt-out of certain cookies by using the opt-out tools provided by third-party advertisers.

Please note that disabling or blocking certain cookies may affect the functionality of our website.

PRIVACY POLICY

Pp

What kind of personal information do you collect from users?

Click all that apply

Email address

First name and last name

Phone number

Address, State, Province, ZIP/Postal code, City

Social Media Profile information (ie. from Connect with Facebook, Sign In With Twitter)

Others

Select additional information you collect from a device (mobile/tablet)

Skip selecting an option if none apply to you

Location (GPS)

Phonebook (Contacts list)

Camera (Pictures)

Do you use tracking and/or analytics tools, such as Google Analytics?

Yes, we use Google Analytics or other related tools

\$24

Select the tools you use for tracking and/or analytics

Click all that apply or add your own

Google Analytics

Firebase

Matomo (formely Piwik)

Clicky

Statcounter

Flurry Analytics

Mixpanel

Unity Analytics

Add Your Own

No

Do you send emails to users?

Yes, we send emails to users or users can opt-in to receive emails from us

\$14

Select the platforms you use to send emails

Click all that apply or add your own

Mailchimp

Constant Contact

AWeber

GetResponse

Add Your Own

No

Do you show ads?

Yes, we show ads

\$24

Select the platforms you use to show ads

Click all that apply

Google Ads (AdSense)

AdMob by Google

Bing Ads

Flurry

InMobi

MoPub

StartApp

AdColony

AppLovin

Vungle

AdButler

Unity Ads

Add Your Own

No

Can users pay for products or services?

Yes, users can pay for our products/services

\$14

Select the payment processors/methods

Click all that apply or add your own

Apple Store In-App Payments

Google Play In-App Payments

PayPal

Braintree

Stripe

FastSpring

Shopify

Square

2Checkout

WePay

WorldPay

Authorize.net

Sage Pay

Go Cardless

Elavon

Verifone

Moneris

WeChat

Alipay

Bank Transfer

Add Your Own

No, we do not sell anything or allow users to pay for products/services

Do you use remarketing services for marketing & advertising purposes?

Yes, we use remarketing services to advertise our business

\$34

Select the platforms you use for remarketing purposes

Click all that apply or add your own

Google Ads (AdWords)

Twitter

Facebook

Bing Ads

Pinterest

AdRoll

Perfect Audience

AppNexus

Add Your Own

No

Select if you use any of the following providers

Skip selecting option if none apply to you

Invisible reCAPTCHA

\$14

Google Places

Mouseflow
FreshDesk

PRIVACY POLICY

A standard privacy policy outlines the website's interactions with users' personal details, which could encompass anything that identifies a specific person, such as:

Name,
Address,
Date of birth,
Marital status,
Contact details,
ID issuance and expiry date,
Financial records,
Credit information,
Medical history,
Travel locations, and
Propensity to purchase goods and services.

Generally, all privacy policies should include at least the following components:

Identity of the website owner or operator,
Details about the type of user data you collect and process, including names, addresses, phone numbers, and email addresses,
Information on how and why you use the data you collect,
Email addresses for marketing, customer service contact information, and shipment addresses,
Methods to maintain the accuracy and relevance of user data,
Means by which you store user data,
Legal grounds for data collection,
Details on if and how you share user data, with whom you share it, including any parent companies and subsidiaries, and any legal obligations to disclose user data,
The third parties that may have access to the data,
When applicable, information about international or cross-border data transfers, including safeguards to ensure safe and legal data transfer,
User rights – can they request access to the information you have about them? Can they request corrections or deletions? and
An outline of the process for notifying users and visitors when the privacy policy is updated.

A GDPR-compliant privacy notice should cover:

Contact details of the Data Protection Officer,
If the organization is not based in the EU but is subject to GDPR, contact information of a representative within the EU,
Information about the legal grounds for data processing and the corresponding reasons,
Data subjects' right to withdraw consent at any moment without negative consequences, where consent has been used as the legal basis,
When legitimate interests are cited as the legal basis for data processing, information about data retention periods for each activity, the legitimate interests pursued by the organization or a third party, the balancing test carried out to balance the organization's legitimate interests with the freedoms and rights of data subjects, and any privacy and security safeguards in place.

Processing of Children's Data

Define the legal age for a child in your country,
Explain in child-friendly language how your organization interacts with parents, what data is collected from minors and shared with others, parental choices and controls, and the duration of data retention.

Sensitive Personal Data Processing

List the categories of sensitive personal data that are collected and processed, the legal basis for such activities, the purposes of collection and processing of sensitive personal data, and the security measures used to protect such data.

Include details on any data processing related to criminal charges and convictions, if applicable.

Automated Individual Decision-making, including Profiling

Specify the types of personal data involved,

Describe the right to object to automated decision-making, including profiling,

Explain the logic behind the automated decision-making process and its impacts,

Detail the appropriate safeguards implemented to protect the rights and freedoms of data subjects.

International Data Transfer

Identify which categories of personal data are transferred to which countries,

Explain the rationale for international data transfer,

State the legal basis of data processing,

Describe the transfer method and how to access or acquire the related document,

Indicate the GDPR article that the organization relies on for the transfer mechanism,

Describe any additional safeguards in place to protect the transferred data.

Data Subject Rights

Provide information about data subject rights and instructions on how to exercise these rights, including the right to information, access, rectification, erasure, restriction of processing, data portability, objection, and the right not to be subject to automated individual decision-making, including profiling.

The California Privacy Rights Act (CPRA)

If your website or online services are utilized by California residents, the rules of the California Privacy Rights Act (CPRA) must be adhered to.

The CPRA isn't confined to companies with physical locations in California. Any company dealing with personal data from customers in California is bound by this law. The CPRA's scope includes:

Companies with an annual gross income exceeding \$25 million,

Companies that purchase, sell, or share personal information of 100,000 or more consumers or households for commercial purposes or derive more than half of their annual revenues from selling customers' personal information.

Just like the California Online Privacy Protection Act (CalOPPA), the CPRA applies to businesses globally.

According to the CPRA, every website must have a privacy policy. Businesses are required to provide consumers with a privacy notice at or before the collection of personal information. This notice must contain information about what categories of personal information the business collects, how it is used, and if it's shared, as well as the reasons for these actions. The privacy policy must also inform consumers about their rights as granted by the CPRA.

A CPRA-compliant privacy policy should include:

Consumer rights under the CPRA,

How California consumers can request access to or deletion of their personal information,

A link to your 'Do Not Sell or Share My Personal Information' page,

The categories of personal information that has been collected in the past 12 months,

The sources of collected personal information,

The reasons for collecting personal information,

Any sold personal information,

The categories of personal information disclosed for business purposes to third parties over the past 12 months,

The categories of personal information sold or shared to third parties in the past 12 months,

Acknowledgement of selling or sharing personal information of consumers under 16 years of age,

If the business knowingly sells personal information of minors, details on how parents or minors can opt-in,

Statement on the use or disclosure of sensitive personal information for purposes other than those specified in CPRA Section 1798.121 and CPRA Regulations 7027(m),

An annual update of the privacy policy,

A clear link to the privacy policy on the website's home page.

Explanation of rights, including:

The right to know,

The right to delete,

The right to correct,

The right to opt-out,

The right to limit the use of sensitive personal information,

The right to non-discrimination.

Description of the methods through which consumers can exercise their rights, what they can expect from these methods, and how they can do so,

Notice of the right to opt-out or a link to it,

Notice of the limit to the use of my sensitive personal information or a link to it,

A brief description of the process the company uses to verify a consumer's request to know, request to delete, and request to correct, where relevant, including any details the consumer is required to provide,

A description of how a consumer's opt-out preference signal will be handled and how the consumer can use an opt-out preference signal.

What data you collect

How it's collected

Why you're collecting the data

Who the information gets shared with, and

What legal basis you have for collecting the data

All rights consumers have under the GDPR

How they can act on those rights

- Introduction explaining the purpose of the privacy policy and its importance.

- Information on the types of personal data collected (e.g., name, email address, IP address).

- Explanation of how personal data is collected (e.g., directly from users, automatically through cookies).

- Purpose of collecting personal data and lawful basis for processing.

- Disclosure of any third parties with whom personal data is shared and the purposes of such sharing.

- Details on how personal data is used, including any marketing or advertising purposes.

- Information on data retention periods and how long personal data is stored.

- Explanation of users' rights regarding their personal data (e.g., right to access, right to rectification, right to erasure).

- How users can exercise their rights and contact the data controller for assistance.

- Security measures in place to protect personal data from unauthorized access or disclosure.

- Any international transfers of personal data and safeguards in place for such transfers.

- Compliance with relevant data protection laws and regulations (e.g., GDPR, CCPA).

- How the privacy policy will be updated and how users will be notified of changes.

- Contact information for questions or concerns about the privacy policy.

Certainly, here are some additional points for a comprehensive privacy policy:

- Explanation of how users can revoke consent for the processing of their personal data.
- Details on the process for handling user requests related to their personal data.
- Any specific data protection measures for sensitive groups such as children or vulnerable individuals.
- Information on how personal data is stored and whether it is stored locally or in the cloud.
- Description of any data anonymization or pseudonymization techniques used to protect user privacy.
- Disclosure of any automated data processing, including the logic involved and potential consequences for users.
- Explanation of how user data is used for research or statistical purposes, if applicable.
- Any restrictions on the transfer of personal data to third countries or international organizations.
- How users can lodge complaints with relevant data protection authorities.
- Details on any data protection impact assessments (DPIAs) conducted by the organization.
- Clarification on whether the organization conducts direct marketing and how users can opt-out.
- Information on any data processing agreements with third-party service providers.
- Description of the organization's approach to data minimization and limiting data collection to what is necessary for the specified purposes.
- Any additional information necessary to comply with industry-specific regulations or standards.
- Clauses addressing the relationship between the organization and its affiliates or subsidiaries regarding data processing activities.
- Any other relevant information to ensure transparency and accountability in the processing of personal data.

A standard privacy policy outlines the website's interactions with users' personal details, which could encompass anything that identifies a specific person, such as:

Name,
 Address,
 Date of birth,
 Marital status,
 Contact details,
 ID issuance and expiry date,
 Financial records,
 Credit information,
 Medical history,
 Travel locations, and
 Propensity to purchase goods and services.

Consumer privacy laws are undergoing changes and becoming more rigorous. Clients and business associates are now asking for detailed information on how companies handle and

protect their customers' personal data. Here are some reasons [why your website requires a privacy policy](#):

- It is a mandatory provision to comply with data privacy laws (GDPR, CCPA, COPPA, etc.),
- It showcases business credibility and fosters trust among customers,
- It reflects transparency and a dedicated security stance,
- It aids in avoiding penalties for non-adherence to laws,
- Third-party apps, analytics apps, and marketing tools require privacy policies,
- It assures that an organization's staff handles data appropriately,
- It sets up internal checks and balances, and
- It diminishes the risk of data exposure and data breach by implementing effective controls.

Key Elements for Crafting Your Website's Privacy Policy

Your privacy policy should be tailored to your platform, accounting for your operational location and business type, as legal requirements can vary between different countries and states.

Depending on the complexity of your business operations, consulting with a lawyer to help you formulate your privacy policy can be beneficial. For example, if you run an online store with international clientele, seeking legal advice can ensure your privacy policy is in accordance with all relevant privacy laws.

Generally, all privacy policies should include at least the following components:

- Identity of the website owner or operator,
- Details about the type of user data you collect and process, including names, addresses, phone numbers, and email addresses,
- Information on how and why you use the data you collect,
- Email addresses for marketing, customer service contact information, and shipment addresses,
- Methods to maintain the accuracy and relevance of user data,

- Means by which you store user data,
- Legal grounds for data collection,
- Details on if and how you share user data, with whom you share it, including any parent companies and subsidiaries, and any legal obligations to disclose user data,
- The third parties that may have access to the data,
- When applicable, information about international or cross-border data transfers, including safeguards to ensure safe and legal data transfer,
- User rights – can they request access to the information you have about them? Can they request corrections or deletions? and
- An outline of the process for notifying users and visitors when the privacy policy is updated.

A GDPR-compliant privacy notice should cover:

- Contact details of the Data Protection Officer,
- If the organization is not based in the EU but is subject to GDPR, contact information of a representative within the EU,
- Information about the legal grounds for data processing and the corresponding reasons,
- Data subjects' right to withdraw consent at any moment without negative consequences, where consent has been used as the legal basis,
- When legitimate interests are cited as the legal basis for data processing, information about data retention periods for each activity, the legitimate interests pursued by the organization or a third party, the balancing test carried out to balance the organization's legitimate interests with the freedoms and rights of data subjects, and any privacy and security safeguards in place.

Processing of Children's Data

- Define the legal age for a child in your country,
- Explain in child-friendly language how your organization interacts with parents, what data is collected from minors and shared with others, parental choices and controls, and the duration of data retention.

Sensitive Personal Data Processing

- List the categories of sensitive personal data that are collected and processed, the legal basis for such activities, the purposes of collection and processing of sensitive personal data, and the security measures used to protect such data.

Include details on any data processing related to criminal charges and convictions, if applicable.

Automated Individual Decision-making, including Profiling

- Specify the types of personal data involved,
- Describe the right to object to automated decision-making, including profiling,
- Explain the logic behind the automated decision-making process and its impacts,
- Detail the appropriate safeguards implemented to protect the rights and freedoms of data subjects.

International Data Transfer

- Identify which categories of personal data are transferred to which countries,
- Explain the rationale for international data transfer,
- State the legal basis of data processing,
- Describe the transfer method and how to access or acquire the related document,
- Indicate the GDPR article that the organization relies on for the transfer mechanism,
- Describe any additional safeguards in place to protect the transferred data.

Data Subject Rights

- Provide information about data subject rights and instructions on how to exercise these rights, including the right to information, access, rectification, erasure, restriction of processing, data portability, objection, and the right not to be subject to automated individual decision-making, including profiling.

A CPRA-compliant privacy policy should include:

- Consumer rights under the CPRA,
- How California consumers can request access to or deletion of their personal information,
- A link to your 'Do Not Sell or Share My Personal Information' page,
- The categories of personal information that has been collected in the past 12 months,
- The sources of collected personal information,
- The reasons for collecting personal information,
- Any sold personal information,
- The categories of personal information disclosed for business purposes to third parties over the past 12 months,
- The categories of personal information sold or shared to third parties in the past 12 months,
- Acknowledgement of selling or sharing personal information of consumers under 16 years of age,
- If the business knowingly sells personal information of minors, details on how parents or minors can opt-in,
- Statement on the use or disclosure of sensitive personal information for purposes other than those specified in CPRA Section 1798.121 and CPRA Regulations 7027(m),
- An annual update of the privacy policy,
- A clear link to the privacy policy on the website's home page.

Explanation of rights, including:

- The right to know,
- The right to delete,
- The right to correct,
- The right to opt-out,
- The right to limit the use of sensitive personal information,
- The right to non-discrimination.

Description of the methods through which consumers can exercise their rights, what they can expect from these methods, and how they can do so,

- Notice of the right to opt-out or a link to it,
- Notice of the limit to the use of my sensitive personal information or a link to it,

A brief description of the process the company uses to verify a consumer's request to know, request to delete, and request to correct, where relevant, including any details the consumer is required to provide,

A description of how a consumer's opt-out preference signal will be handled and how the consumer can use an opt-out preference signal.

Common Elements for GDPR and CPRA-Compliant Privacy Notice

Both GDPR and CPRA-compliant privacy notices should include:

The name, identity, and contact information of the data controller,

Details of data processing activities including:

- The categories of personal information to be collected,
- The purposes of data processing (specific business or commercial purpose),
- Data retention periods, where precise durations of data should be explicitly stated. If the duration isn't mentioned, the criteria used to determine the retention period should be mentioned,
- The source, or categories of sources, from which personal data is collected if not directly gathered from the subject.

Data Sharing, including:

- The individuals or groups who received personal information when it was sold or shared.
Provide categories of recipients or actual (named) recipients of the personal data, as applicable,
- A clear business or commercial reason for the sale or transfer of customer data,
- Types of third parties who received the information,
- A clear business or commercial purpose for disclosing the customer's personal data.

Cookies, including:

- The data subject's right to opt-in and opt-out of cookies,
- The explanation that essential cookies will always remain enabled,
- The right of the data subject to withdraw and update their consent, and the procedure for doing so (cookie preference center),
- The purposes of cookies,
- The data retention periods,
- Whether or not third parties can access personal data via cookies,
- Where applicable, details on appropriate safeguards and any potential risks associated with cross-border data transfers via cookies.

A clear description of data security measures implemented by the business to ensure data confidentiality,

The data subject's right to lodge a complaint with the relevant regulatory authority against the organization for violating their rights,

The date the privacy policy was last updated must be explicitly stated,

The individual's name and their contact details for any questions or concerns about the business's privacy policies.

What is CalOPPA

CalOPPA came into law on 1 July 2004 and covers operators of commercial websites that collect personally identifiable information. Its main requirement is that these website operators **must conspicuously link to a Privacy Policy on their website.**

The Privacy Policy required by CalOPPA law must also have certain clauses, including:

- What types of personal information is collected and the third parties this collected personal information may be shared with
- How users can request changes to any of the personally identifiable information that was collected
- How the operator will notify users of changes/updates to the Privacy Policy
- The effective date of the Privacy Policy
- How the operator responds to the "Do Not Track" requests of users

- Whether other third parties may collect personally identifiable information about users through the operator's service

2.2 Information we collect about you.

- **Contact Information (for example an email address).**

You might provide us with your contact information, whether through use of our services, a form on our website, an interaction with our sales or customer support team, or a response to one of SurveyMonkey's own surveys.

- **Usage information.**

We collect usage information about you whenever you interact with our websites and services. This includes which webpages you visit, what you click on, when you perform those actions, what language preference you have, and so on.

- **Device and browser data.**

We collect information from the device and application you use to access our services. Device data mainly means your IP address, operating system version, device type, system and performance information, and browser type. If you are on a mobile device we also collect the UUID for that device.

- **Information from page tags.**

We use third party tracking services that employ cookies and page tags (also known as [web beacons](#)) to collect data about visitors to our websites. This data includes usage and user statistics. Emails sent by SurveyMonkey or by users through our services include page tags that allow the sender to collect information about who opened those emails and clicked on links in them. We provide more information on cookies [below](#) and in our [Cookies Policy](#).

- **Log Data.**

Like most websites today, our web servers keep log files that record data each time a device accesses those servers. The log files contain data about the nature of each access, including originating IP addresses, internet service providers, the files viewed on our site (e.g., HTML pages, graphics, etc.), operating system versions, device type and timestamps.

When and why do we share this information with third parties?

- Shopify works with a variety of third parties and service providers to help provide you with our Services and we may share personal information with them to support these efforts.
- We may also share your information in the following circumstances:
 - to prevent, investigate, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our Terms of Service or any other agreement related to the Services, or as otherwise required by law.
 - to help us conduct marketing and/or advertising campaigns.
 - to conform to legal requirements, or to respond to lawful court orders, subpoenas, warrants, or other requests by public authorities (including to meet national security or law enforcement requirements).
- Personal information may also be shared with a company that acquires our business, whether through merger, acquisition, bankruptcy, dissolution, reorganization, or other similar transaction or proceeding. If this happens, we will post a notice on our home page.
- Shopify will always ask for your consent before sharing your personal information with third parties for purposes other than those described in this Section 2.
- Shopify is responsible for all onward transfers of personal information to third parties in accordance with the EU-U.S. Privacy Shield Framework, the Swiss-U.S. Privacy Shield Framework, and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

Accessing and Updating Information

All users and customers of LivingClean.com may access, update, or delete their personal information at any time by logging into their [account settings](#).

We can also provide information upon request as to what personal data is stored about you. In addition, we will correct or erase personal data at your request, with the exception of data retained for legal obligations. To learn more or to make any of the requests described above, email us at privacy@livingclean.com.

Notice Concerning Do Not Track

Do Not Track ("DNT") is a privacy preference that users can set in certain web browsers. We are committed to providing you with meaningful choices about the information collected on our website for third party purposes, and that is why we provide the variety of opt-out mechanisms listed above. However, we do not currently recognize or respond to browser-initiated DNT signals. To learn more about Do Not Track, you can do so [here](#).

EFFECTIVE DAAAAAAAAAAAAATE UPDATEEEEEEEEEES

Clickwrap is a much stronger method of getting consent to your legal agreements (regardless if it's a Privacy Policy or not) where the links are posted alongside a checkbox or a button that explicitly states "I Agree" which informs users that they're entering into an agreement:

Key Definitions In the GDPR

Now that you know the GDPR basics, I suggest you familiarize yourself with the legal definitions of several key phrases used in the regulation to help simplify your compliance process.

In the table below, I show you the definition of those essential words as it appears in the GDPR and provide a simplified version of the meanings.

Term	Precise Legal Definition	Simplified Definition
Personal data	<p><i>“... any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”</i></p> <p>(Chapter 1, Article 4, Part 1)</p>	<p>Information about a person that can directly or indirectly identify them, like:</p> <ul style="list-style-type: none">• Names• E-mail address• ID numbers• Addresses• Precise geolocation• IP addresses• Biometric data• Sensitive personal information

<p>Processing</p>	<p>“... any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;”</p> <p>(Chapter 1, Article 4, Part 2)</p>	<p>Doing any of the following actions to a piece or set of personal data:</p> <ul style="list-style-type: none"> • Collecting • Recording • Organizing • Structuring • Storing • Adapting • Altering • Retrieving • Consulting • Using • Disclosing • Disseminating • Making available • Aligning • Combining • Restricting • Erasing • Destroying
<p>Consent</p>	<p>“...any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;”</p> <p>(Chapter 1, Article 4, Part 11)</p>	<p>When a data subject freely agrees to data processing by taking an affirmative, clear action (like selecting a checkbox, clicking a button labeled ‘I Agree’, writing it on a piece of paper, or signing a document with this purpose) and has access to and read a compliant privacy policy that informs them about the entity’s data processing activities.</p> <p>*This is an important definition to pay attention to if your business relies on consent as a legal basis for processing personal data</p>

Data controller	<p><i>“...the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;”</i></p> <p>(Chapter 1, Article 4, Part 7)</p>	<p>Any natural person or entity that determines the reason for and means of processing personal data pertaining to data subjects (e.g., customers, users, website visitors, etc.).</p>
Data processor	<p>a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;</p> <p>(Chapter 1, Article 4, Part 8)</p>	<p>Any third party tasked by a data controller to process personal data based on the instructions provided by the controller and on their behalf.</p>

Conditions for Legally Processing Personal Data

To lawfully process personal data under the GDPR, you must state your legal basis for each category of information you use.

The GDPR outlines the following legal bases as compliant reasons for data processing:

Consent: You can rely on consent only if you offer data subjects control and genuine choice for accepting or declining the terms offered without detriment to your processing activities. You must also follow specific conditions outlined by the GDPR to have a valid lawful basis for collecting personal information. Because this is a common legal basis for businesses, we cover it in greater detail in the next section.

Contractual performance: If the processing is necessary for the performance of a contract that includes the data subject, then this is a legitimate reason for processing user information.

Legitimate interest: If processing the data is necessary for your legitimate interests, then this legal basis applies unless these legitimate interests override the rights and freedoms of the data subjects concerned.

Vital interest: This applies in life or death situations and refers to processing necessary data to protect the vital interests of a data subject.

Legal requirement: This legal basis applies when processing is necessary to fulfill a legal obligation.

Public interest: This applies when processing data is necessary to perform a task in the general public's interest and typically applies to public entities or private entities that perform a task in the public interest.

How Personal Information Is Defined by Data Privacy Laws

There are many examples of personal information listed above, but you must know what specific laws govern your business and how they define personal information.

The table below gives a brief overview of some legal definitions of the term, and later, we'll explain them in more detail.

Law or Regulation	Region	Definition of Personal Information
Australian Privacy Principles (Privacy Act 1988)	Australia	Any information that can (or reasonably could) identify a living individual.
California Consumer Privacy Act (CCPA)	California	Any information, within reason, that is linked with a distinguishable person or household.
California Privacy Rights Act (CPRA)	California	Added sensitive information to CCPA's personal information.
California Online Privacy Protection Act (CalOPPA)	California	Specific list of data types (see below).
Consumer Data Protection Act (CDPA)	Virginia	Information linked or reasonably linkable to an identified or identifiable natural person.

Colorado Privacy Act (CPA)	Colorado	Any information, within reason, that is linked with a distinguishable person. Does not include de-identified data.
Connecticut Personal Data Privacy and Online Monitoring Act (CTDPA)	Connecticut	any information that is linked or reasonably linkable to an identified or identifiable individual. Does not include de-identified or publicly available information.
General Data Protection Regulation (GDPR)	European Union	Information that can lead to the identification of a person — i.e., credit card number, email address, name, etc.
Personal Information Protection and Electronic Documents Act (PIPEDA)	Canada	Information about an identifiable individual.

You can read the full definition according to the GDPR here:

Any information relating to an identified or identifiable natural person, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The California Consumer Privacy Act ([CCPA](#)) applies to anyone who services residents of California and meets certain thresholds.

It defines personal information as:

Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

Fundamentals of Privacy Policies

Ready for a bit of privacy policy history? Privacy policies are based on by-laws established by the U.S. Federal Trade Commission in 1998.

Also known as [fair information practice principles](#) (FIPPs), these by-laws note that privacy policies must include five fundamental aspects:

- Notice: Consumers must be notified of a platform's practices regarding personal information before it's collected from them
- Choice: Consumers should be able to have a choice about personal data collection and use
- Access: Consumers must have access to their personal data
- Security: A company must protect the personal information it collects, have a process to delete old data, safeguard current user data and disclose its security practices in a privacy policy
- Enforcement: Enforcement measures on how these principles will be implemented must be made clear

Many laws and regulations have updated these guidelines since 1998, but the basic principles still make up the foundation for data privacy in the US.

1. About this Policy

This Privacy Policy describes how we process your personal data at Spotify USA Inc. From now on, we'll call it the 'Policy'.

It applies to your use of:

- all Spotify streaming services as a user. For example this includes:
 - your use of Spotify on any device
 - the personalization of your user experience. Watch [our personalization explainer video](#) to learn more about this
 - the infrastructure required to provide our services
 - connection of your Spotify account with another application
 - both our free or paid streaming options (each a 'Service Option')
- other Spotify services which include a link to this Policy. These include Spotify websites, Customer Service and the Community Site

From now on, we'll collectively call these the 'Spotify Service'.

Personal Data Apple Collects from You



At Apple, we believe that you can have great products and great privacy. This means that we strive to **collect only the personal data that we need**. Descriptions of how Apple handles personal data for certain individual services are available at apple.com/legal/privacy/data.

When you create an Apple ID, apply for commercial credit, purchase and/or activate a product or device, download a software update, register for a class at an Apple Store, connect to our services, contact us (including by social media), participate in an online survey, or otherwise interact with Apple, we may collect a variety of information, including:

- **Account Information.** Your Apple ID and related account details, including email address, devices registered, account status, and age
- **Device Information.** Data from which your device could be identified, such as device serial number, or about your device, such as browser type
- **Contact Information.** Data such as name, email address, physical address, phone number, or other contact information
- **Payment Information.** Data about your billing address and method of payment, such as bank details, credit, debit, or other payment card information
- **Transaction Information.** Data about purchases of Apple products and services or transactions facilitated by Apple, including purchases on Apple platforms
- **Fraud Prevention Information.** Data used to help identify and prevent fraud, including a device trust score
- **Usage Data.** Data about your activity on and use of our offerings, such as app launches within our services, including browsing history; search history; product interaction; crash data, performance and other diagnostic data; and other usage data
- **Location Information.** Precise location only to support services such as Find My or where you agree for region-specific services, and coarse location

HOW WE COLLECT YOUR INFORMATION



We collect information you provide to us when you request or purchase products, services, or information from us, register with us (including when you link your profile on a third-party site or platform with your registration account), participate in [public forums](#) or other activities on our sites and applications, respond to guest surveys, visit our physical properties, call our reservation centers or other guest services phone numbers, or otherwise interact with us using one or more devices. You may provide information in a variety of ways, including by typing or using voice commands.

We collect information through a variety of technologies, such as cookies, Flash cookies, pixels, tags, software development kits, [application](#) program interfaces, and Web beacons, including when you visit our sites and applications or use our applications on third-party sites or platforms using one or more devices, whether or not you are logged in or registered. Please visit [Online Tracking Technologies and Advertising](#) for further information, including Do Not Track and how to disable cookies and otherwise make choices with respect to such data collection.

Purpose for processing your data	Legal basis that permits the purpose	Categories of personal data used for the purpose
<p>To provide the Spotify Service in accordance with our contract with you.</p> <p>For example, when we use your personal data to:</p> <ul style="list-style-type: none"> • set up an account for you • personalize your account, or • provide the Spotify app when you download it onto your device 	<p>Performance of a Contract</p>	<ul style="list-style-type: none"> • User Data • Street Address Data • Usage Data • Voice Data • Payment and Purchase Data
<p>To provide further parts of the Spotify Service.</p> <p>For example, when we use your personal data to enable you to share a link to Spotify content with someone else.</p>	<p>Legitimate Interest</p> <p>Our legitimate interests here include:</p> <ul style="list-style-type: none"> • keeping the Spotify Service running and functional • allowing users to access and use the Spotify Service 	<ul style="list-style-type: none"> • User Data • Street Address Data • Usage Data • Voice Data • Payment and Purchase Data
<p>To provide certain additional voluntary features of the Spotify Service. When this is the case, we will clearly ask for your consent.</p>	<p>Consent</p>	<ul style="list-style-type: none"> • User Data • Usage Data • Survey and Research Data • Payment and Purchase Data

- **Power Our Services.** Apple collects personal data necessary to power our services, which may include personal data collected to improve our offerings, for internal purposes such as auditing or data analysis, or for troubleshooting. For example, if you would like to access a song through an Apple Music subscription, we collect data on what songs you play in order to provide you with the content requested and for royalty purposes.
- **Process Your Transactions.** To process transactions, Apple must collect data such as your name, purchase, and payment information.
- **Communicate with You.** To respond to communications, reach out to you about your transactions or account, market our products and services, provide other relevant information, or request information or feedback. From time to time, we may use your personal data to send important notices, such as communications about purchases and changes to our terms, conditions, and policies. Because this information is important to your interaction with Apple, you may not opt out of receiving these important notices.
- **Security and Fraud Prevention.** To protect individuals, employees, and Apple and for loss prevention and to prevent fraud, including to protect individuals, employees, and Apple for the benefit of all our users, and prescreening or scanning uploaded content for potentially illegal content, including child sexual exploitation material.
- **Personal Data Used for Personalization.** If you choose to personalize your services or communications where such options are available, Apple will use information that we collect so that we can offer you those personalized services or communications. You can learn more about how relevant services use information to personalize your experience by reviewing the privacy information presented when you first use a service that asks to use your personal data. We make this information easy to find by presenting it with our Data & Privacy icon; it's also available at all times on your Apple device and online at apple.com/legal/privacy/data.
- **Comply with Law.** To comply with applicable law — for example, to satisfy tax or reporting obligations, or to comply with a lawful governmental request.

When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

With your consent

We'll share personal information outside of Google when we have your consent. For example, if you [use Google Home to make a reservation](#) through a booking service, we'll get your permission before sharing your name or phone number with the restaurant. We also provide you with controls to [review and manage third party apps and sites](#) you have given access to data in your Google Account. We'll ask for your explicit consent to share any [sensitive personal information](#).

With domain administrators

If you're a student or work for an organization that uses Google services, your [domain administrator](#) and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email
- View statistics regarding your account, like how many apps you install
- Change your account password
- Suspend or terminate your account access
- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

We recognize the need to provide further privacy protections with respect to personal information we may collect from children on our sites and applications. Some of the features on our sites and applications are age-gated so that they are not available for use by children, and we do not knowingly collect personal information from children in connection with those features. When we intend to collect personal information from children, we take additional steps to protect children's privacy, including:

- Notifying parents about our information practices with regard to children, including the types of personal information we may collect from children, the uses to which we may put that information, and whether and with whom we may share that information;
- In accordance with applicable law, and our practices, obtaining consent from parents for the collection of personal information from their children, or for sending information about our products and services directly to their children;
- Limiting our collection of personal information from children to no more than is reasonably necessary to participate in an online activity; and
- Giving parents access or the ability to request access to personal information we have collected from their children and the ability to request that the personal information be changed or deleted.

For additional information about our practices in the United States regarding children's personal information, please read our [Children's Privacy Policy](#).

IV. Choice and transparency

Uber enables users to access and/or control data that Uber collects, including through:

- *privacy settings*
- *device permissions*
- *in-app ratings pages*
- *marketing choices*

Uber also enables users to request access to or copies of their data, make changes or updates to their accounts, request deletion of their accounts, or request that Uber restrict its processing of user data.

A. Privacy settings

The Settings > Privacy menu in the Uber app allows riders and order recipients to set or update their preferences regarding location data collection and sharing, emergency data sharing, and notifications. Our [Privacy Center](#) is also available in web version.

- **Location data collection (riders and order recipients)**

Riders and order recipients can enable/disable Uber to collect location data from their mobile devices through their device settings, which can be accessed via the Settings > Privacy > Location menu.

- **Share Live Location (Riders)**

Riders can enable/disable Uber to share their real-time location data from their mobile devices with their drivers through their device settings, which can be accessed via the Settings > Privacy > Location menu.

✓ Information Security and Data Retention

We use physical, technical, organizational, and administrative safeguards to help protect your Personal Information from unauthorized access or loss. For example, we use encryption and other tools to protect sensitive information. We retain your Personal Information as needed for the purposes listed above and as permitted by law.

RETAINING YOUR INFORMATION

We retain the data we collect for different periods of time depending on what it is, how we use it, and how you configure your settings:

- Some data you can delete whenever you like, such as your [personal info](#) or the content you create or upload, like [photos](#) and [documents](#). You can also delete [activity information](#) saved in your account, or [choose to have it deleted automatically](#) after a set period of time. We'll keep this data in your Google Account until you remove it or choose to have it removed.
- Other data is deleted or anonymized automatically after a set period of time, such as [advertising data](#) in server logs.
- We keep some data until you delete your Google Account, such as information about how often you use our services.
- And some data we retain for longer periods of time when necessary for legitimate business or legal purposes, such as security, fraud and abuse prevention, or financial record-keeping.

C. Cookies and third-party technologies

Uber and its partners use cookies and other identification technologies on our apps, websites, emails, and online ads for purposes described in this notice, and Uber's [Cookie Notice](#).

Cookies are small text files that are stored on browsers or devices by websites, apps, online media, and advertisements. Uber uses cookies and similar technologies for purposes such as:

- authenticating users
- remembering user preferences and settings
- determining the popularity of content
- delivering and measuring the effectiveness of advertising campaigns
- analyzing site traffic and trends, and generally understanding the online behaviors and interests of people who interact with our services

We may also allow others to provide audience measurement and analytics services for us, to serve advertisements on our behalf across the internet, and to track and report on the performance of those advertisements. These entities may use cookies, web beacons, SDKs, and other technologies to identify the devices used by visitors to our websites, as well as when they visit other online sites and services.

Please see our [Cookie Notice](#) for more information regarding the use of cookies and other technologies described in this section.

How will you know the policy has changed?

We'll notify you before we make material changes to this Policy. You'll have the opportunity to review the revised Policy before you choose to continue using our Products.

[Links to](#)

[Other Policies](#)

It's a business best practice to link to other relevant legal and website policies within your privacy policy, primarily your:

- [Terms and conditions](#)
- [Cookie policy](#)
- [Disclaimers](#) or [warranties](#)

4. What types of personal information does the BBC collect about me?

We'll give you details about why we need your personal information and how we'll use it before you begin, unless it's obvious.

a. Information that you give us

We might ask for your name and contact details, your date of birth or financial details, depending on what you're doing. If you apply to take part in a programme on politics, for example, we might ask you about your political opinions. Information you give us might include information in a [creation](#) you share with us, such as people's names that appear in the creation.

When you [register for a BBC account](#), or update your details or settings we ask for some personal information, like your email address and age.

b. Device information

Devices are lots of things like:

- your computer
- your mobile
- your TV
- your tablet
- your voice-enabled device

We [automatically collect some technical information from these devices and web browsers](#) even when you're not signed into to a [BBC account](#). This might include:

- IP (internet protocol) address
- device ID
- app ID
- vendor ID
- advertising ID

c. Location Information

We collect information about your location when you use our products and services. This helps us to determine whether you're somewhere where services are available, helps us to ensure we are fulfilling our Charter obligations and to offer additional features whilst using our products and services, such as a weather forecast for your location.

Your location can be determined at a town or city level by:

- GPS
- IP address
- Information about nearby cell towers and Wi-Fi access point information

What type of location data (for example Country, Region, City or Town) is collected depends on the product or service you're using, the device you're using (for example Apple or Android) and your device's settings (whether permissions are enabled or disabled). You can change your permissions on or off any time in your device's settings. You can read more about [how our apps capture your data on our explainers](#).

d. Information on your activities outside the BBC when you talk about us

Like if you've mentioned us in a Twitter post, we'll collect your Twitter handle.

e. Information on how you use our services

Like [the articles you read and the programmes you watch](#).

[BACK TO TOP](#)

How we use your information

Uber puts transportation, food delivery, and other services at your fingertips. Understanding what data we collect and how we use it should be just as easy.

Our [Privacy Notice](#) explains in detail what data we collect and how we use it to provide you with a safe and reliable user experience.

We've also summarized this information in the charts below. These show for each category of Uber users (Riders, Order Recipients, and Drivers/Delivery Persons) the purposes for which Uber uses data, and the types of data we use for each purpose.

You can also [download an expanded version](#) of this chart.

How to read this table

- ✓ means that we use the data for this purpose globally
- ✓* means that we use the data for this purpose globally, other than in the European Economic Area / the United Kingdom and Switzerland

These charts also indicate the legal basis that Uber relies on for each use of data under privacy laws such as the European Union's General Data Protection Regulation.

- Consent (C)
- Contractual Necessity (CN)
- Legitimate Interest (LI)
- Legal Obligation (LO)

Data Categories	Rider	Order Recipients	Drivers and Delivery Persons
To provide our services	+		
For safety and security	+		
For customer support	+		
For research and development	+		
To enable communications between users	+		
For marketing	+		
For non-marketing communications	+		
For legal proceedings and requirement	+		

DATA SECURITY, INTEGRITY, AND RETENTION

The security, integrity, and confidentiality of your information are extremely important to us. We have implemented technical, administrative, and physical security measures that are designed to protect guest information from unauthorized access, disclosure, use, and modification. We regularly review our security procedures to consider appropriate new technology and methods. Please be aware that, despite our best efforts, no security measures are perfect or impenetrable. We will retain your personal information for the length of time needed to fulfill the purposes outlined in this privacy policy unless a longer retention period is required or permitted by law.

9. When does the BBC share my personal information with others?

We share your information with others in these ways:

a. When you make something public

Like [post a comment](#) which the public can see.

b. When we use other companies to power our services

In order for us to give you quality experiences and to understand how you're using our services we often use other companies to process [your personal information](#) on our behalf.

For example, sending you emails about things we think might interest you, or analysing data on how people use our digital services so we can improve them.

We make sure that your personal information is looked after as if we were handling it directly. We carefully select these companies, only share with them what they need to do the work and we make sure they [keep your information secure](#).

c. When advertising companies buy ad space and personalise their advertising

We work with a range of advertising and data companies to sell and deliver ads, and keep track of how they did. Some of these ads are personalised. Generally, these companies act as separate data controllers, or they might control your data on behalf of their advertiser client rather than us. We don't share your account data with them.

d. When we share personal information with companies in the BBC family

[BBC Studios](#) and the BBC PSB work together on features like BBC account, and understanding how BBC services are used globally. This means that some information is shared between us.

e. When we do collaborative research

The BBC PSB sometimes collaborates with research partners. Every now and then we share data with them. This might include information we've collected about you. But we're careful about what we share and what BBC research partners can do with it.

f. Sometimes by law we have to pass on your information to other organisations

We might also share your information if we have to by law, or when we need to protect you or other people from harm.

[BACK TO TOP](#)

C. Cookies and third-party technologies

Uber and its partners use cookies and other identification technologies on our apps, websites, emails and online ads for purposes described in this notice, and [Uber's Cookie Notice](#).

Cookies are small text files that are stored on browsers or devices by websites, apps, online media and advertisements. Uber uses cookies and similar technologies for purposes such as:

- authenticating users
- remembering user preferences and settings
- determining the popularity of content
- delivering and measuring the effectiveness of advertising campaigns
- analysing site traffic and trends, and generally understanding the online behaviours and interests of people who interact with our services

We may also allow others to provide audience measurement and analytics services for us, to serve advertisements on our behalf across the internet and to track and report on the performance of those advertisements. These entities may use cookies, web beacons, SDKs and other technologies to identify the devices used by visitors to our websites, as well as when they visit other online sites and services.

Please see our [Cookie Notice](#) for more information regarding the use of cookies and other technologies described in this section.

NOTICE OF COLLECTION OF PERSONAL INFORMATION

We collect these categories of personal information when you interact with us: identifiers/contact information, demographic information (such as gender and age), payment card information associated with you, commercial information, Internet or other electronic network activity information, geolocation data, audio, electronic, visual or similar information, and inferences drawn from the above.

We collect this information so that we can best serve you, including to fulfill your requests and to share offers that we think you may be interested in. A more detailed description of these purposes is in our Privacy Policy under "[USE OF YOUR INFORMATION BY THE WALT DISNEY FAMILY OF COMPANIES](#)."

California residents also have the right to "**OPT OUT**" of the "sale" of their "personal information" to "third parties" (as those terms are defined in the CCPA and described below).

15. How can I contact the BBC?

Find out more and [contact us about your rights](#).

For any other questions or comments about this policy contact to our Data Protection Officer:

- [by email](#)
- by post: Data Protection Officer, Regulatory Affairs, BBC Studios, 1 Television Centre, 101 Wood Lane, London W12 7FA

If you're in the UK, please contact the BBC Public Service Data Protection Officer:

- [by email](#)
- by post at BBC Data Protection Officer, C/o First Floor, Wogan House, 99 Great Portland Street, London, W1W 7NY

We're regulated by the [Information Commissioner's Office](#). You can also contact them for advice and support.

[BACK TO TOP](#)

Additional

Many businesses require additional clauses in their privacy policies. Read through the following list and make a note of any sections that are relevant to your website.

Transferring Information Internationally

If you transfer data you've collected internationally, insert a business transfer clause into your privacy policy. The GDPR limits transferring personal data outside of Europe unless the other country has safeguards or is considered safe.

Data Retention

Some privacy policies have a data retention clause outlining how long the information is kept or stored. According to the GDPR, you should store data only for as long as necessary. But this information can also be included in other clauses of your policy, like how Disney incorporated it into their data security clause pictured above.

Collecting Information from Minors

Collecting information from minors under 13 requires additional regulations in adherence with laws like COPPA. You must include a clause expressing how you use the information you are gathering about children, and you need parent or guardian consent.

Below, see another example privacy policy photo from Disney, this time the clause clearly outlines the data collection protections they put in place to protect children, and provides a link to their COPPA-compliant children's privacy policy.

CHILDREN'S PRIVACY

—

We recognize the need to provide further privacy protections with respect to personal information we may collect from children on our sites and applications. Some of the features on our sites and applications are age-gated so that they are not available for use by children, and we do not knowingly collect personal information from children in connection with those features. When we intend to collect personal information from children, we take additional steps to protect children's privacy, including:

- Notifying parents about our information practices with regard to children, including the types of personal information we may collect from children, the uses to which we may put that information, and whether and with whom we may share that information;
- In accordance with applicable law, and our practices, obtaining consent from parents for the collection of personal information from their children, or for sending information about our products and services directly to their children;
- Limiting our collection of personal information from children to no more than is reasonably necessary to participate in an on-line activity; and
- Giving parents access or the ability to request access to personal information we have collected from their children and the ability to request that the personal information be changed or deleted.

For additional information about our practices in the United States regarding children's personal information, [please read our CHILDREN'S PRIVACY POLICY](#).

Handling Social Media Logins

Websites and apps that use pre-existing social media logins also require an additional clause. In this case, your privacy policy must inform your user what data you share with those third parties, why, and how it gets used.

User Rights Over Their Data

Different laws outline data privacy rights consumers can legally act on, like opting out of the sale of data under the CCPA or opting into different personal data tracking under the GDPR.

Include a clause informing users of the process they can follow to act on their privacy rights.

Do-Not-Track Features and Controls

The GDPR and CCPA grant users the right to request access, change, or delete any data gathered about them.

Add a clause in your transparent privacy policy about DNT features and controls and state how your business responds to this type of request from users.

Special Privacy Rights for California Residents

To simplify CCPA compliance, many companies include a separate clause outlining the specific data privacy rights granted to California residents.

Links to Other Legal Documents

To make it easy on your consumers and to ensure they always have access to all necessary legal agreements, link those other documents within the clauses of your privacy policy.

For example, link to your cookie policy under the Cookies and Other Trackers clause in your privacy agreement.

You can even link to your privacy policy within those other legal documents, like your [terms and conditions](#) or [disclaimer](#), this way you ensure your users can always find, access, and read all of your legal policies.

Definition of Sensitive Personal Information

Sensitive personal information, sometimes called SPI, is data that is subject to strict protection guidelines under laws like the GDPR and the CCPA and includes very intimate details, such as:

- Political affiliations
- Religious beliefs
- Philosophical beliefs
- Race or ethnicity
- Sexual orientation
- Health data
- Biometric data
- Criminal history
- Credit or financial data
- Trade union and membership information
- Personal identification (ID) numbers — license, social security, state ID cards, passports

Some laws set stricter guidelines for collecting, using, and securely storing this type of information because of the vulnerable nature of the data.

If SPI is compromised or breached, it could cause permanent harm to the individual's quality of life or impact their ability to perform daily activities, so it's essential to follow all relevant legal guidelines if you deal with sensitive user data.

The Differences Between Personal vs. Sensitive Information

The differences between personal and sensitive information are subtle, but SPI is technically a distinct category of personal data that you must treat, store, and handle differently based on applicable privacy laws.

Broadly speaking, personal information refers to any data that can directly or indirectly identify a person or household.

Personal information can include any of the following details:

- Names
- Email addresses
- Mailing addresses
- IP addresses
- Phone numbers
- Dates of birth
- ZIP codes
- Sensitive information

But SPI, by nature, is more vulnerable than other personal identifiers.

Sensitive personal data examples include:

- A person's beliefs
- Medical and genetic data
- Criminal histories
- Opinions
- Sexual identity
- Race
- Other more intimate details

If either type of data is leaked, it could harm the affected individuals, but the unauthorized access of sensitive data is particularly harmful as it could lead to:

- Discrimination
- Harassment
- Identity theft
- Other types of permanent harm

Therefore, different data privacy laws dictate how businesses can legally collect, store, and use such delicate information and grant users more rights over that data.

What Is Considered Sensitive Personal Information?

Take a look at the table below to see a list of examples of sensitive personal data and the relevant privacy laws that include it in their legal definition of SPI.

Applicable Data Privacy Law(s)	Type of Sensitive Personal Information
<ul style="list-style-type: none">• GDPR• CCPA• Australian Privacy Act	<ul style="list-style-type: none">• Political opinions or affiliations
<ul style="list-style-type: none">• GDPR• CCPA• Virginia CDPA• Australian Privacy Act	<ul style="list-style-type: none">• Religious or philosophical beliefs
<ul style="list-style-type: none">• GDPR• CCPA• Virginia CDPA	<ul style="list-style-type: none">• Race or ethnic origins

<ul style="list-style-type: none"> • GDPR • CCPA • Australian Privacy Act 	<ul style="list-style-type: none"> • Trade union membership
<ul style="list-style-type: none"> • GDPR • CCPA • Virginia CDPA • Australian Privacy Act 	<ul style="list-style-type: none"> • Medical or health data
<ul style="list-style-type: none"> • GDPR • CCPA • Virginia CDPA • Australian Privacy Act 	<ul style="list-style-type: none"> • Genetics data
<ul style="list-style-type: none"> • GDPR • CCPA • Virginia CDPA • Australian Privacy Act 	<ul style="list-style-type: none"> • Biometric data
<ul style="list-style-type: none"> • GDPR • CCPA • Virginia CDPA • Australian Privacy Act 	<ul style="list-style-type: none"> • Sexual orientation or sex life
<ul style="list-style-type: none"> • Australian Privacy Act 	<ul style="list-style-type: none"> • Criminal records
<ul style="list-style-type: none"> • Virginia CDPA 	<ul style="list-style-type: none"> • Citizenship or immigration status

<ul style="list-style-type: none"> • CCPA 	<ul style="list-style-type: none"> • Personal ID numbers (social security, driver's license, passport, state ID)
<ul style="list-style-type: none"> • CCPA 	<ul style="list-style-type: none"> • Account login data
<ul style="list-style-type: none"> • CCPA 	<ul style="list-style-type: none"> • Credit or debit card number (in combination with relevant credentials to access an account)
<ul style="list-style-type: none"> • CCPA 	<ul style="list-style-type: none"> • Precise geolocation
<ul style="list-style-type: none"> • Virginia CDPA 	<ul style="list-style-type: none"> • Data collected from known children

What Is Not Considered Sensitive Personal Information?

Depending on what privacy laws you fall under, the following details might not qualify as sensitive personal information:

- Publicly available information from federal, state, or local government records.
- Lawfully obtained, truthful information that is a matter of public concern.
- Information a business has a reasonable basis to believe is made lawfully available to the general public by the consumer or by widely distributed media.

- Information made available by a person to whom the consumer has disclosed the data if the consumer has not restricted that information to a specific audience.

However, what is and isn't considered SPI can change from one law to another.

PRIVACY POLICY

Last updated [Date]

This privacy notice for [Company Name] (doing business as [Company Short Name]) ("we," "us," or "our"), describes how and why we might collect, store, use, and/or share ("process") your information when you use our services ("Services"), such as when you:

- Visit our website at [Website URL], or any website of ours that links to this privacy notice
- [Download and use our application(s), such as our mobile application – [Mobile App Name], [our Facebook application – [Facebook App Name],] or any other application of ours that links to this privacy notice]
- Engage with us in other related ways – including any sales, marketing, or events

Questions or concerns? Reading this privacy policy will help you understand your privacy rights and choices. If you do not agree with our policies and practices, please do not use our Services. If you still have any questions or concerns, please contact us at [Email Address].

I. DEFINITIONS

For the purposes of this Privacy Policy, except where a different definition is noted, "personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California consumer/resident or household. Personal information does not include publicly available information, information that has been de-identified or aggregated, or other information covered by certain sector-specific privacy laws.

Term	Precise Legal Definition	Simplified Definition
Personal data	<i>"... any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic,</i>	Information about a person that can directly or indirectly identify them, like: <ul style="list-style-type: none">• Names• E-mail address• ID numbers• Addresses• Precise geolocation• IP addresses• Biometric data

	<p><i>cultural or social identity of that natural person;”</i></p> <p>(Chapter 1, Article 4, Part 1)</p>	<ul style="list-style-type: none"> • Sensitive personal information
Processing	<p><i>“... any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;”</i></p> <p>(Chapter 1, Article 4, Part 2)</p>	<p>Doing any of the following actions to a piece or set of personal data:</p> <ul style="list-style-type: none"> • Collecting • Recording • Organizing • Structuring • Storing • Adapting • Altering • Retrieving • Consulting • Using • Disclosing • Disseminating • Making available • Aligning • Combining • Restricting • Erasing • Destroying

<p>Consent</p>	<p><i>“...any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;”</i></p> <p>(Chapter 1, Article 4, Part 11)</p>	<p>When a data subject freely agrees to data processing by taking an affirmative, clear action (like selecting a checkbox, clicking a button labeled ‘I Agree’, writing it on a piece of paper, or signing a document with this purpose) and has access to and read a compliant privacy policy that informs them about the entity’s data processing activities.</p> <p>*This is an important definition to pay attention to if your business relies on consent as a legal basis for processing personal data</p>
<p>Data controller</p>	<p><i>“...the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;”</i></p> <p>(Chapter 1, Article 4, Part 7)</p>	<p>Any natural person or entity that determines the reason for and means of processing personal data pertaining to data subjects (e.g., customers, users, website visitors, etc.).</p>
<p>Data processor</p>	<p>a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; (Chapter 1, Article 4, Part 8)</p>	<p>Any third party tasked by a data controller to process personal data based on the instructions provided by the controller and on their behalf.</p>

II. CCPA DISCLOSURES AND RIGHTS

A. Personal Information We Collect

BeatStars may collect, or has collected, the following categories of personal information about you over the last twelve (12) months:

Identifiers, which includes your name and username; birthday; email address, mailing address, and telephone number; online identifiers as detailed below including IP address or device IDs; name, and password; government-issued identification card number; and/or other similar identifiers.

Payment and financial information, including your credit or debit card number, PayPal email address, and/or other financial information.

Commercial information, which includes records of music recordings; products or services including subscriptions purchased, obtained, or considered; participation in working with Sony Music Publishing; account balances, payment history, or account activity; bank account information and other information relating to your financial institution; and/or other purchasing or consumer histories or tendencies.

Information relating to Internet activity or other electronic network activity, which includes your browsing history and Site usage information, interactions with ads, IP address, cookie identifiers, clear gifs (web beacons/web bugs), browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp, device platform, and device version.

Geolocation data, which includes Global Positioning System ("GPS") data based on your IP address.

Audio, electronic, or visual information, which includes music recordings, images and comment that you or others submit to our Site to be featured, displayed, or streamed on our Site; and recordings of calls to or from our customer service centers.

Inferences drawn from personal information listed above which includes preferences, such as your listening preferences, interests and other information, used create a profile about you in order for us to personalize ads and content.

Information not listed above and related to characteristics protected under California or federal law, which may include gender, if you display it on your profile or elsewhere on the platform.

We at OpenAI OpCo, LLC (together with our affiliates, "OpenAI", "we", "our" or "us") respect your privacy and are strongly committed to keeping secure any information we obtain from you or about you. This Privacy Policy describes our practices with respect to Personal Information we collect from or about you when you use our website, applications, and services (collectively, "Services"). This Privacy Policy does not apply to content that we process on behalf of customers of our business offerings, such as our API. Our use of that data is governed by our customer agreements covering access to and use of those offerings.

For information about how we collect and use training information to develop our language models that power ChatGPT and other Services, and your choices with respect to that information, please see this help center article([opens in a new window](#)).

SUMMARY OF KEY POINTS

This summary provides key points from our privacy notice, but you can find out more details about any of these topics by clicking the link following each key point or by using our [table of contents](#) below to find the section you are looking for.

What personal information do we process? When you visit, use, or navigate our Services, we may process personal information depending on how you interact with us and the Services, the choices you make, and the products and features you use. Learn more about [personal information you disclose to us](#).

Do we process any sensitive personal information? [We do not process sensitive personal information. / We may process sensitive personal information when necessary with your consent or as otherwise permitted by applicable law. Learn more about [sensitive information we process.](#)]

Do we receive any information from third parties? We may receive information from public databases, marketing partners, social media platforms, and other outside sources. Learn more about [information collected from other sources.](#)

How do we process your information? We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent. We process your information only when we have a valid legal reason to do so. Learn more about [how we process your information.](#)

In what situations and with which types of parties do we share personal information? We may share information in specific situations and with specific categories of third parties. Learn more about [when and with whom we share your personal information.](#)

How do we keep your information safe? We have organizational and technical processes and procedures in place to protect your personal information. However, no electronic transmission over the internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security and improperly collect, access, steal, or modify your information. Learn more about [how we keep your information safe.](#)

What are your rights? Depending on where you are located geographically, the applicable privacy law may mean you have certain rights regarding your personal information. Learn more about [your privacy rights.](#)

How do I exercise my rights? The easiest way to exercise your rights is by filling out our data subject access request form available here: [\[DSAR Form URL\]](#), or by contacting us. We will consider and act upon any request in accordance with applicable data protection laws.

Want to learn more about what we do does with any information we collect? [Review the privacy notice in full.](#)

TABLE OF CONTENTS

[1. WHAT INFORMATION DO WE COLLECT?](#)

[2. HOW DO WE PROCESS YOUR INFORMATION?](#)

[3. WHAT LEGAL BASES DO WE RELY ON TO PROCESS YOUR PERSONAL INFORMATION?](#)

[4. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?](#)

[5. WHAT IS OUR STANCE ON THIRD-PARTY WEBSITES?](#)

[6. DO WE USE COOKIES AND OTHER TRACKING TECHNOLOGIES?](#)

[7. HOW DO WE HANDLE YOUR SOCIAL LOGINS?](#)

[8. IS YOUR INFORMATION TRANSFERRED INTERNATIONALLY?](#)

[9. HOW LONG DO WE KEEP YOUR INFORMATION?](#)

[10. HOW DO WE KEEP YOUR INFORMATION SAFE?](#)

[11. DO WE COLLECT INFORMATION FROM MINORS?](#)

[12. WHAT ARE YOUR PRIVACY RIGHTS?](#)

[13. CONTROLS FOR DO-NOT-TRACK FEATURES](#)

[14. DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?](#)

[15. DO OTHER REGIONS HAVE SPECIFIC PRIVACY RIGHTS?](#)

[16. DO WE MAKE UPDATES TO THIS NOTICE?](#)

[17. HOW CAN YOU CONTACT US ABOUT THIS NOTICE?](#)

[18. HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?](#)

1. WHAT INFORMATION DO WE COLLECT?

Personal information you disclose to us

***In Short:** We collect personal information that you provide to us.*

We collect personal information that you voluntarily provide to us when you [\[register on the Services,\]](#) express an interest in obtaining information about us or our products and Services, when you participate in activities on the Services, or otherwise when you contact us.

Personal Information Provided by You. The personal information that we collect depends on the context of your interactions with us and the Services, the choices you make, and the products and features you use. The personal information we collect may include the following:

- [\[Personal Info Collected\]](#)
- [\[Personal Info Collected\]](#)
- [\[Personal Info Collected\]](#)

Sensitive Information. [\[We do not process sensitive information. / When necessary, with your consent or as otherwise permitted by applicable law, we process the following categories of sensitive information:](#)

- [Sensitive Info Collected]
- [Sensitive Info Collected]
- [Sensitive Info Collected]]

Payment Data. We may collect data necessary to process your payment if you make purchases, such as your payment instrument number (such as a credit card number), and the security code associated with your payment instrument. All payment data is stored by [Vendor Name]. You may find their privacy notice link(s) here: [Vendor Privacy Policy].

Social Media Login Data. We may provide you with the option to register with us using your existing social media account details, like your Facebook, Twitter, or other social media account. If you choose to register in this way, we will collect the information described in the section called "[HOW DO WE HANDLE YOUR SOCIAL LOGINS?](#)" below.

[Application Data. If you use our application(s), we also may collect the following information if you choose to provide us with access or permission:

- *Geolocation Information.* We may request access or permission to track location-based information from your mobile device, either continuously or while you are using our mobile application(s), to provide certain location-based services. If you wish to change our access or permissions, you may do so in your device's settings.
- *Mobile Device Access.* We may request access or permission to certain features from your mobile device, including your mobile device's bluetooth, calendar, camera, own, and other features. If you wish to change our access or permissions, you may do so in your device's settings.
- *Mobile Device Data.* We automatically collect device information (such as your mobile device ID, model, and manufacturer), operating system, version information and system configuration information, device and application identification numbers, browser type and version, hardware model Internet service provider and/or mobile carrier, and Internet Protocol (IP) address (or proxy server). If you are using our application(s), we may also collect information about the phone network associated with your mobile device, your mobile device's operating system or platform, the type of mobile device you use, your mobile device's unique device ID, and information about the features of our application(s) you accessed.
- *Push Notifications.* We may request to send you push notifications regarding your account or certain features of the application(s). If you wish to opt out from receiving these types of communications, you may turn them off in your device's settings.

This information is primarily needed to maintain the security and operation of our application(s), for troubleshooting, and for our internal analytics and reporting purposes.]

B. What We Do With Your Information

BeatStars may collect, use, or disclosure personal information about you for the following purposes:

Provide our Services to you (such as account registration) and maintain the Platform and your account;
Market and sell our products and services;
Bill you for services and process subscription payments;
Provide you with a personalized content and ads;
Operate and maintain safe, secure and reliable Services and Sites;
Improve our operational efficiency and provide you with better products and services;
Perform research and development;
Contact you in response to an inquiry that you sent;
Send you messages and information related to our products and services, support and administrative messages, technical notices, updates, alerts, and other information;
Send you information about services and programs we offer that may be of interest to you;
Recommend artists to our business partners for publishing engagements;
Detect and prevent fraud and abuse, including perform identity verification;
Perform accounting, audits and other internal functions; and
Comply with request or order from courts, law enforcement or other government authorities.
BeatStars may also use personal information for other business purposes, including the following: (i) perform accounting, audits and other internal functions; (ii) compliance with our legal obligations or to assert or defend a legal claim; (iii) general business administration; (iii) processing employment applications; and (iv) systems and data security.

C. Sources of Collected Information

We may collect personal information from the following categories of sources:

From you, including via our Sites, telephone, postal mail, social media, forums, or other means
Business partnersthat promote and/or offer services
Advertising networks
Social networkswith whom you choose to connect your BeatStars account to
Other third parties, which includes payment portals you opt to use outside of those authorized by us, operators of other websites and mobile applications, and other data suppliers
Other sources, including things that other third parties may post publicly about you or otherwise provide to us
We may supplement the information described above with information we obtain from other sources, including from both online and offline data providers.

1. Personal information we collect

We collect personal information relating to you ("Personal Information") as follows:

Personal information you provide: We collect Personal Information if you create an account to use our Services or communicate with us as follows:

Account Information: When you create an account with us, we will collect information associated with your account, including your name, contact information, account credentials, payment card information, and transaction history, (collectively, "Account Information").

User Content: When you use our Services, we collect Personal Information that is included in the input, file uploads, or feedback that you provide to our Services ("Content").

Communication Information: If you communicate with us, we collect your name, contact information, and the contents of any messages you send ("Communication Information").

Social Media Information: We have pages on social media sites like Instagram, Facebook, Medium, Twitter, YouTube and LinkedIn. When you interact with our social media pages, we will collect Personal Information that you elect to provide to us, such as your contact details (collectively, “Social Information”). In addition, the companies that host our social media pages may provide us with aggregate information and analytics about our social media activity.

Other Information You Provide: We collect other information that you may provide to us, such as when you participate in our events or surveys or provide us with information to establish your identity (collectively, “Other Information You Provide”)

Personal information we receive automatically from your use of the Services: When you visit, use, or interact with the Services, we receive the following information about your visit, use, or interactions (“Technical Information”):

Log Data: Information that your browser or device automatically sends when you use our Services. Log data includes your Internet Protocol address, browser type and settings, the date and time of your request, and how you interact with our Services.

Usage Data: We may automatically collect information about your use of the Services, such as the types of content that you view or engage with, the features you use and the actions you take, as well as your time zone, country, the dates and times of access, user agent and version, type of computer or mobile device, and your computer connection.

Device Information: Includes name of the device, operating system, device identifiers, and browser you are using. Information collected may depend on the type of device you use and its settings.

Cookies: We use cookies to operate and administer our Services, and improve your experience. A “cookie” is a piece of information sent to your browser by a website you visit. You can set your browser to accept all cookies, to reject all cookies, or to notify you whenever a cookie is offered so that you can decide each time whether to accept it. However, refusing a cookie may in some cases preclude you from using, or negatively affect the display or function of, a website or certain areas or features of a website. For more details on cookies, please visit [All About Cookies](#)(opens in a new window).

Analytics: We may use a variety of online analytics products that use cookies to help us analyze how users use our Services and enhance your experience when you use the Services.

All personal information that you provide to us must be true, complete, and accurate, and you must notify us of any changes to such personal information.

Information automatically collected

In Short: Some information – such as your Internet Protocol (IP) address and/or browser and device characteristics – is collected automatically when you visit our Services.

We automatically collect certain information when you visit, use, or navigate the Services. This information does not reveal your specific identity (like your name or contact information) but may include device and usage information, such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, country, location, information about how and

when you use our Services, and other technical information. This information is primarily needed to maintain the security and operation of our Services, and for our internal analytics and reporting purposes.

Like many businesses, we also collect information through cookies and similar technologies. You can find out more about this in our Cookie Notice: [\[Cookie Notice URL\]](#).

The information we collect includes:

- *Log and Usage Data.* Log and usage data is service-related, diagnostic, usage, and performance information our servers automatically collect when you access or use our Services and which we record in log files. Depending on how you interact with us, this log data may include your IP address, device information, browser type, and settings and information about your activity in the Services (such as the date/time stamps associated with your usage, pages and files viewed, searches, and other actions you take such as which features you use), device event information (such as system activity, error reports (sometimes called "crash dumps"), and hardware settings).
- *Device Data.* We collect device data such as information about your computer, phone, tablet, or other device you use to access the Services. Depending on the device used, this device data may include information such as your IP address (or proxy server), device and application identification numbers, location, browser type, hardware model, Internet service provider and/or mobile carrier, operating system, and system configuration information.
- *Location Data.* We collect location data such as information about your device's location, which can be either precise or imprecise. How much information we collect depends on the type and settings of the device you use to access the Services. For example, we may use GPS and other technologies to collect geolocation data that tells us your current location (based on your IP address). You can opt out of allowing us to collect this information either by refusing access to the information or by disabling your Location setting on your device. However, if you choose to opt out, you may not be able to use certain aspects of the Services.
- [\[Other\]](#)

Information collected from other sources

In Short: We may collect limited data from public databases, marketing partners, social media platforms, and other outside sources.

In order to enhance our ability to provide relevant marketing, offers, and services to you and update our records, we may obtain information about you from other sources, such as public databases, joint marketing partners, affiliate programs, data providers, social media platforms, and from other third parties. This information includes mailing addresses, job titles, email addresses, phone numbers, intent

data (or user behavior data), Internet Protocol (IP) addresses, social media profiles, social media URLs, and custom profiles, for purposes of targeted advertising and event promotion. If you interact with us on a social media platform using your social media account (e.g., Facebook or Twitter), we receive personal information about you such as your name, email address, and gender. Any personal information that we collect from your social media account depends on your social media account's privacy settings.

[Information collected when you use our Facebook application(s). We by default access your Facebook basic account information, including your name, email, gender, birthday, current city, and profile picture URL, as well as other information that you choose to make public. We may also request access to other permissions related to your account, such as friends, check-ins, and likes, and you may choose to grant or deny us access to each individual permission. For more information regarding Facebook permissions, refer to the [Facebook Permissions Reference](#) page.]

2. HOW DO WE PROCESS YOUR INFORMATION?

***In Short:** We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent.*

We process your personal information for a variety of reasons, depending on how you interact with our Services, including:

- **To facilitate account creation and authentication and otherwise manage user accounts.** We may process your information so you can create and log in to your account, as well as keep your account in working order.
- **To deliver and facilitate delivery of services to the user.** We may process your information to provide you with the requested service.
- **To respond to user inquiries/offer support to users.** We may process your information to respond to your inquiries and solve any potential issues you might have with the requested service.
- **To send administrative information to you.** We may process your information to send you details about our products and services, changes to our terms and policies, and other similar information.
- **To fulfill and manage your orders.** We may process your information to fulfill and manage your orders, payments, returns, and exchanges made through the Services.
- **To enable user-to-user communications.** We may process your information if you choose to use any of our offerings that allow for communication with another user.

- **To request feedback.** We may process your information when necessary to request feedback and to contact you about your use of our Services.
- **To send you marketing and promotional communications.** We may process the personal information you send to us for our marketing purposes, if this is in accordance with your marketing preferences. You can opt out of our marketing emails at any time. For more information, see "[WHAT ARE YOUR PRIVACY RIGHTS?](#)" below).
- **To deliver targeted advertising to you.** We may process your information to develop and display personalized content and advertising tailored to your interests, location, and more. For more information see our Cookie Notice: [\[Cookie Notice URL\]](#).
- **To protect our Services.** We may process your information as part of our efforts to keep our Services safe and secure, including fraud monitoring and prevention.
- **To identify usage trends.** We may process information about how you use our Services to better understand how they are being used so we can improve them.
- **To determine the effectiveness of our marketing and promotional campaigns.** We may process your information to better understand how to provide marketing and promotional campaigns that are most relevant to you.
- **To save or protect an individual's vital interest.** We may process your information when necessary to save or protect an individual's vital interest, such as to prevent harm.
- [\[Other\]](#)

E. Data Protection

This Data Protection section applies to all users of any services owned or controlled by Beatstars Inc. Furthermore, this section extends to Service Providers, Contractors, Affiliates, Vendors, Affiliates, Agents, and Entities; their parent company and subsidiaries, or their respective employees, officers, directors, members, managers, shareholders, agents, vendors, licensors, licensees, contractors, customers, successors, and assigns (each referred to as "Parties" in the following paragraph). By executing any Agreement with Beatstars Inc., which uses any personal information, Parties agree to abide by the following paragraph. Violation of this section is cause for termination of Service or rights granted by Beatstars, Inc. Moreover, if an agreement has been executed between Beatstars Inc. and a Party, violation of this section is considered a material breach.

Each party shall, at its own expense, ensure that it complies with and assists Beatstars Inc. to comply with the requirements of all legislation and regulatory requirements in force from time to time relating to the use of personal data, including (without limitation) (i) any U.S Data Protection legislation, including but not limited to the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). This clause is in addition to, and does not reduce, remove or replace, a party's obligations arising from such requirements hereunder. You confirm that you will not rent or sell customer lists, contact details or other data without the customers' express prior approval.

2. How we use personal information

We may use Personal Information for the following purposes:

To provide, administer, maintain and/or analyze the Services;

To improve our Services and conduct research;

To communicate with you; including to send you information about our Services and events;

To develop new programs and services;

To prevent fraud, criminal activity, or misuses of our Services, and to protect the security of our IT systems, architecture, and networks;

To carry out business transfers; and

To comply with legal obligations and legal process and to protect our rights, privacy, safety, or property, and/or that of our affiliates, you, or other third parties.

Aggregated or de-identified information. We may aggregate or de-identify Personal Information so that it may no longer be used to identify you and use such information to analyze the effectiveness of our Services, to improve and add features to our Services, to conduct research and for other similar purposes. In addition, from time to time, we may analyze the general behavior and characteristics of users of our Services and share aggregated information like general user statistics with third parties, publish such aggregated information or make such aggregated information generally available. We may collect aggregated information through the Services, through cookies, and through other means described in this Privacy Policy. We will maintain and use de-identified information in anonymous or de-identified form and we will not attempt to reidentify the information, unless required by law.

As noted above, we may use Content you provide us to improve our Services, for example to train the models that power ChatGPT. Read our instructions([opens in a new window](#)) on how you can opt out of our use of your Content to train our models.

3. Disclosure of personal information

In certain circumstances we may provide your Personal Information to third parties without further notice to you, unless required by the law:

Vendors and Service Providers: To assist us in meeting business operations needs and to perform certain services and functions, we may provide Personal Information to vendors and service providers, including providers of hosting services, customer service vendors, cloud services, email communication software, web analytics services, and other information technology providers, among others. Pursuant to our instructions, these parties will access, process, or store Personal Information only in the course of performing their duties to us.

Business Transfers: If we are involved in strategic transactions, reorganization, bankruptcy, receivership, or transition of service to another provider (collectively, a “Transaction”), your Personal Information and other information may be disclosed in the diligence process with counterparties and others assisting with the Transaction and transferred to a successor or affiliate as part of that Transaction along with other assets.

Legal Requirements: We may share your Personal Information, including information about your interaction with our Services, with government authorities, industry peers, or other third parties (i) if required to do so by law or in the good faith belief that such action is necessary to comply with a legal obligation, (ii) to protect and defend our rights or property, (iii) if we determine, in our sole discretion, that there is a violation of our terms,

policies, or the law; (iv) to detect or prevent fraud or other illegal activity; (v) to protect the safety, security, and integrity of our products, employees, or users, or the public, or (vi) to protect against legal liability.

Affiliates: We may disclose Personal Information to our affiliates, meaning an entity that controls, is controlled by, or is under common control with OpenAI. Our affiliates may use the Personal Information we share in a manner consistent with this Privacy Policy.

Business Account Administrators: When you join a ChatGPT Enterprise or business account, the administrators of that account may access and control your OpenAI account. In addition, if you create an account using an email address belonging to your employer or another organization, we may share the fact that you have an OpenAI account and certain account information, such as your email address, with your employer or organization to, for example, enable you to be added to their business account.

Other Users and Third Parties You Share Information With: Certain features allow you to display or share information with other users or third parties. For example, you may share ChatGPT conversations with other users via shared links or send information to third-party applications via custom actions for GPTs. Be sure you trust any user or third party with whom you share information.

5. Additional U.S. state disclosures

The following table provides additional information about the categories of Personal Information we collect and how we disclose that information. You can read more about the Personal Information we collect in “Personal information we collect” above, how we use Personal Information in “How we use personal information” above, and how we retain Personal Information in “Security and Retention” below.

Category of Personal Information	Disclosure of Personal Information
Identifiers, such as your name, contact details, IP address, and other device identifiers	We may disclose this information to our affiliates, vendors and service providers to process in accordance with our instructions; to law enforcement and other third parties for the legal reasons described above; to parties involved in Transactions; to corporate administrators of enterprise or team accounts; and to other users and third parties you choose to share it with.
Commercial Information, such as your transaction history	We may disclose this information to our affiliates, vendors and service providers to process in accordance with our instructions; to law enforcement and other third parties for the legal reasons described above; to parties involved in Transactions; and to corporate administrators of enterprise or team accounts.
Network Activity Information, such as Content and how you interact with our Services	We may disclose this information to our affiliates, vendors and service providers to process in accordance with our instructions; to law enforcement and other third parties for the legal reasons described above; to parties involved in Transactions; and to other users and third parties you choose to share it with.
Geolocation Data	We may disclose this information to our affiliates, vendors and service providers to process in accordance with our instructions; to law enforcement and other third parties for the legal reasons described above; and to parties involved in Transactions.
Your account login credentials and payment card information (Sensitive Personal Information)	

We disclose this information to our affiliates, vendors and service providers, law enforcement, and parties involved in Transactions.

To the extent provided for by local law and subject to applicable exceptions, individuals may have the following privacy rights in relation to their Personal Information:

The right to know information about our processing of your Personal Information, including the specific pieces of Personal Information that we have collected from you;

The right to request deletion of your Personal Information;

The right to correct your Personal Information; and

The right to be free from discrimination relating to the exercise of any of your privacy rights.

We don't "sell" Personal Information or "share" Personal Information for cross-contextual behavioral advertising (as those terms are defined under applicable local law). We also don't process sensitive Personal Information for the purposes of inferring characteristics about a consumer.

Exercising your rights. To the extent applicable under local law, you can exercise privacy rights described in this section by submitting a request through privacy.openai.com (opens in a new window) or to dsar@openai.com.

Verification. In order to protect your Personal Information from unauthorized access, change, or deletion, we may require you to verify your credentials before you can submit a request to know, correct, or delete Personal Information. If you do not have an account with us, or if we suspect fraudulent or malicious activity, we may ask you to provide additional Personal Information and proof of residency for verification. If we cannot verify your identity, we will not be able to honor your request.

Authorized agents. You may also submit a rights request through an authorized agent. If you do so, the agent must present signed written permission to act on your behalf and you may also be required to independently verify your identity and submit proof of your residency with us. Authorized agent requests can be submitted to dsar@openai.com.

Appeals. Depending on where you live, you may have the right to appeal a decision we make relating to requests to exercise your rights under applicable local law. To appeal a decision, please send your request to dsar@openai.com.

3. WHAT LEGAL BASES DO WE RELY ON TO PROCESS YOUR INFORMATION?

In Short: We only process your personal information when we believe it is necessary and we have a valid legal reason (i.e., legal basis) to do so under applicable law, like with your consent, to comply with laws, to provide you with services to enter into or fulfill our contractual obligations, to protect your rights, or to fulfill our legitimate business interests.

If you are located in the EU or UK, this section applies to you.

The General Data Protection Regulation (GDPR) and UK GDPR require us to explain the valid legal bases we rely on in order to process your personal information. As such, we may rely on the following legal bases to process your personal information:

- **Consent.** We may process your information if you have given us permission (i.e., consent) to use your personal information for a specific purpose. You can withdraw your consent at any time. Learn more about [withdrawing your consent](#).
- **Performance of a Contract.** We may process your personal information when we believe it is necessary to fulfill our contractual obligations to you, including providing our Services or at your request prior to entering into a contract with you.
- **Legitimate Interests.** We may process your information when we believe it is reasonably necessary to achieve our legitimate business interests and those interests do not outweigh your interests and fundamental rights and freedoms. For example, we may process your personal information for some of the purposes described in order to:
 - Send users information about special offers and discounts on our products and services
 - Develop and display personalized and relevant advertising content for our users
 - Analyze how our Services are used so we can improve them to engage and retain users
 - Support our marketing activities
 - Diagnose problems and/or prevent fraudulent activities
 - Understand how our users use our products and services so we can improve user experience
 - [\[Other\]](#)
- **Legal Obligations.** We may process your information where we believe it is necessary for compliance with our legal obligations, such as to cooperate with a law enforcement body or regulatory agency, exercise or defend our legal rights, or disclose your information as evidence in litigation in which we are involved.
- **Vital Interests.** We may process your information where we believe it is necessary to protect your vital interests or the vital interests of a third party, such as situations involving potential threats to the safety of any person.

In legal terms, we are generally the “data controller” under European data protection laws of the personal information described in this privacy notice, since we determine the means and/or purposes of the data processing we perform. This privacy notice does not apply to the personal information we process as a “data processor” on behalf of our customers. In those situations, the customer that we provide services to and with whom we have entered into a data processing agreement is the “data controller” responsible for your personal information, and we merely process your information on their behalf in accordance with your instructions. If you want to know more about our customers' privacy practices, you should read their privacy policies and direct any questions you have to them.

GDPR Privacy Notice

Effective date: 28/07/2022

The purpose of the General Data Protection Regulation ("GDPR") is to protect all European Union ("EU") citizens from privacy and data breaches by allowing citizens to maintain control of the personal data kept and processed by organizations, which includes BeatStars Inc ("BeatStars", "us", "we", or "our") . The GDPR also protects the personal data of individuals, regardless of citizenry, in the EU.

BeatStars is committed to safeguarding the privacy of personal data. Furthermore, BeatStars is committed to protecting your privacy online. We are also committed to providing you with the very best experience we can on our website at BeatStars.com and BeatStars mobile (our "Sites") and all related sites and other web-based services that enable website visitor access on our behalf, including players, widgets, tools and other services provided by BeatStars (collectively, the "Services"). This Policy also describes how we use personal data, the purpose for sharing and recipients of personal data and your rights and choices associated with that data. By using BeatStars, you are consenting to the practices described in this Privacy Notice.

Use of Information

Our primary goal in collecting personal information is to provide you, the user, with a customized experience on our website. We use the collected data for various purposes including:

- To provide and maintain our Sites and Services, including to take steps to enter into a contract for sale or services, bill you for services and process payments and fulfill transactions;
- To enable and allow you to participate in interactive features of our Sites and Services and provide you with a personalized service, content and ads;
- To create custom audiences on social media sites;
- To provide you with better products and services and improve and grow our business, including to perform research and development, understand our customer base and purchasing trends and understand the effectiveness of our marketing;
- To operate and maintain safe, secure and reliable Sites and Services;
- To provide customer support, including to contact you in response to an inquiry that you sent, and send administrative messages, technical notices, updates, alerts and other information;
- To provide you with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless you have opted not to receive such information;
- To track the progress and number of entries in our promotions and contests;
- To contact you on behalf of certain artists or other third parties and recommend artists to our business partners for publishing engagements;
- To perform accounting, audits and other internal functions; and
- To comply with a request or order from courts, law enforcement or other government authorities.

BeatStars may also use personal information for other business purposes, including the following: (i) perform accounting, audits and other internal functions; (ii) compliance with our legal obligations or to assert or defend a legal claim; (iii) general business administration; (iii) processing employment applications; and (iv) systems and data security.

In addition, if we feel that a user abuses the BeatStars.com site in any way, we reserve the right to use and share certain information with third parties. Abuses include (but are not limited to) possible copyright infringement, possible libel and slander, and possible fraudulent or illegal activity.

Third Party Use of Sensitive Information

We may disclose your Sensitive Information and other Information as follows:

Consent: We may disclose Information if we have your consent to do so.

Emergency Circumstances: We may share your Information when necessary to protect your interests and you are physically or legally incapable of providing consent.

Employment Necessity: We may share your Information when necessary for administering employment or social security benefits in accordance with applicable law or any applicable collective bargaining agreement, subject to the imposition of appropriate safeguards to prevent further unauthorized disclosure.

Public Information: We may share your Information if you have manifestly made it public.

Archiving: We may share your Information for archival purposes in the public interest, and for historical research and statistical purposes.

Performance of a Contract: We may share your Information when necessary to administer a contract you have with the BeatStars.

Legal Obligation: We may share your Information when the disclosure is required or permitted by international, federal, and state laws and regulations.

Service Providers: We use third parties who have entered into a contract with the BeatStars. In such cases, we share your Information with such third parties subject to the imposition of appropriate safeguards to prevent further unauthorized disclosure.

BeatStars Affiliates: We may share your Information with parties that are affiliated with the BeatStars for the purpose of contacting you about goods, services, charitable giving or experiences that may be of interest to you.

De-Identified and Aggregate Information: We may use and disclose Information in de-identified or aggregate form without limitation.

Security

We implement appropriate technical and organizational security measures to protect your information when you transmit it to us and when we store it on our information technology systems.

Cookies and Other Technology

The BeatStars use of cookies and other data can be found in the BeatStars' Privacy Policy.

Retention and Destruction of Your Information

Your information will be retained by the BeatStars in accordance with applicable state and federal laws, and the applicable retention periods in the Privacy Policy. Your information will be destroyed upon your request unless applicable law requires destruction after the expiration of an applicable retention period. The manner of destruction shall be appropriate to preserve and ensure the confidentiality of your information given the level of sensitivity, value and criticality to the BeatStars.

Your Rights

You have the right to request access to, a copy of, rectification, restriction in the use of, or erasure of your information in accordance with all applicable laws. The erasure of your information shall be subject to applicable state and federal laws, and the applicable retention periods in the BeatStars Privacy Policy. If you have provided consent to the use of your information, you have the right to withdraw consent without affecting the lawfulness of the BeatStars' use of the information prior to receipt of your request.

Information created in the European Union will be transferred out of the European Union to the BeatStars. If you feel BeatStars has not complied with applicable foreign laws regulating such information, you have the right to file a complaint with the appropriate supervisory authority in the European Union.

Updates to This Policy

We may update or change this policy at any time. Your continued use of the BeatStars' website and third party applications after any such change indicates your acceptance of these changes.

Contact Us

If you have any questions about this GDPR Policy or wish to exercise one of your Data Subject rights, please contact us:

By emailing us: ;

By visiting [page](#) on our website.

If you are located in Canada, this section applies to you.

We may process your information if you have given us specific permission (i.e., express consent) to use your personal information for a specific purpose, or in situations where your permission can be inferred (i.e., implied consent). You can withdraw your consent at any time. Click [here](#) to learn more.

In some exceptional cases, we may be legally permitted under applicable law to process your information without your consent, including, for example:

- If collection is clearly in the interests of an individual and consent cannot be obtained in a timely way
- For investigations and fraud detection and prevention
- For business transactions provided certain conditions are met
- If it is contained in a witness statement and the collection is necessary to assess, process, or settle an insurance claim
- For identifying injured, ill, or deceased persons and communicating with next of kin
- If we have reasonable grounds to believe an individual has been, is, or may be victim of financial abuse
- If it is reasonable to expect collection and use with consent would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province
- If disclosure is required to comply with a subpoena, warrant, court order, or rules of the court relating to the production of records
- If it was produced by an individual in the course of their employment, business, or profession and the collection is consistent with the purposes for which the information was produced
- If the collection is solely for journalistic, artistic, or literary purposes
- If the information is publicly available and is specified by the regulations

4. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?

In Short: We may share information in specific situations described in this section and/or with the following categories of third parties.

Vendors, Consultants, and Other Third-Party Service Providers. We may share your data with third-party vendors, service providers, contractors, or agents (“**third parties**”) who perform services for us or on our behalf and require access to such information to do that work. We have contracts in place with our third parties, which are designed to help safeguard your personal information. This means that they cannot do

anything with your personal information unless we have instructed them to do it. They will also not share your personal information with any organization apart from us. They also commit to protect the data they hold on our behalf and to retain it for the period we instruct. The categories of third parties we may share personal information with are as follows:

- Ad Networks
- Affiliate Marketing Programs
- Cloud Computing Services
- Communication & Collaboration Tools
- Data Analytics Services
- Data Storage Service Providers
- Finance & Accounting Tools
- Government Entities
- Order Fulfillment Service Providers
- Payment Processors
- Performance Monitoring Tools
- Product Engineering & Design Tools
- Retargeting Platforms
- Sales & Marketing Tools
- Social Networks
- Testing Tools
- User Account Registration & Authentication Services
- Website Hosting Service Providers
- [\[Other\]](#)

We also may need to share your personal information in the following situations:

- **Business Transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.
- **When we use Google Analytics.** We may share your information with Google Analytics to track and analyze the use of the Services. The Google Analytics Advertising Features that we may use include: [\[List Features\]](#). To opt out of being tracked by Google Analytics across the Services, visit <https://tools.google.com/dlpage/gaoptout>. You can opt out of Google Analytics Advertising Features through [Ads Settings](#) and Ad Settings for mobile apps. Other opt out means include <http://optout.networkadvertising.org/> and <http://www.networkadvertising.org/mobile-choice>. For more information on the privacy practices of Google, please visit the [Google Privacy & Terms page](#).

- **When we use Google Maps Platform APIs.** We may share your information with certain Google Maps Platform APIs (e.g., Google Maps API, Places API). To find out more about Google's Privacy Policy, please refer to this [link](#). We use certain Google Maps Platform APIs to retrieve certain information when you make location-specific requests. This includes: [\[List of Information Collected\]](#), and other similar information. A full list of what we use information for can be found in this section and in the previous section titled "[HOW DO WE PROCESS YOUR INFORMATION?](#)" [\[We obtain and store on your device \("cache"\) your location for \[#\] months. You may revoke your consent anytime by contacting us at the contact details provided at the end of this document.\]](#)
The Google Maps Platform APIs that we use store and access cookies and other information on your devices. If you are a user currently in the European Economic Area (EU countries, Iceland, Liechtenstein and Norway) or the United Kingdom, please take a look at our Cookie Notice, which can be found at this link: [\[Cookie Notice URL\]](#).
- **Affiliates.** We may share your information with our affiliates, in which case we will require those affiliates to honor this privacy notice. Affiliates include our parent company and any subsidiaries, joint venture partners, or other companies that we control or that are under common control with us.
- **Business Partners.** We may share your information with our business partners to offer you certain products, services, or promotions.
- **Other Users.** When you share personal information (for example, by posting comments, contributions, or other content to the Services) or otherwise interact with public areas of the Services, such personal information may be viewed by all users and may be publicly made available outside the Services in perpetuity. If you interact with other users of our Services and register for our Services through a social network (such as Facebook), your contacts on the social network will see your name, profile photo, and descriptions of your activity. Similarly, other users will be able to view descriptions of your activity, communicate with you within our Services, and view your profile.
- **[Offer Wall.** Our application(s) may display a third-party hosted "offer wall." Such an offer wall allows third-party advertisers to offer virtual currency, gifts, or other items to users in return for the acceptance and completion of an advertisement offer. Such an offer wall may appear in our application(s) and be displayed to you based on certain data, such as your geographic area or demographic information. When you click on an offer wall, you will be brought to an external website belonging to other persons and will leave our application(s). A unique identifier, such as your user ID, will be shared with the offer wall provider in order to prevent fraud and properly credit your account with the relevant reward.]

D. Who We Share Your Information With

We limit our disclosure of the categories of personal information above to our service providers for one or more business purposes. We may also provide your personal identifiers such as name, email address, and phone number to our business partners, but not limited to including Sony Music Publishing, for consideration for potential publishing when you have expressly directed us to do so by filling out a publishing application.

We do not sell your personal information to third parties, including personal information of minors under 16 years of age. As with nearly every e-commerce company, we do share a limited set of data that is gathered when you visit our Site, such as cookies and pixels, with third parties in order to allow you to see tailored digital advertisements. To the extent this activity is interpreted as included in California's broad definition of "data sale", we have provided you with opt-out rights as to that activity as described in Section II(f) below.

In the last twelve (12) months, we've disclosed certain personal information to the following categories of third parties:

Categories of third parties	Categories of personal information disclosed
Other users and artists through the Services, including artists	

Identifiers; audio, electronic, or visual information; and information related to characteristics protected under California or federal law

Business partners such as Sony Music Publishing

Identifiers; commercial information; and audio, electronic, or visual information

Advertising partners

Identifiers; information relating to Internet activity or other electronic network activity; geolocation data; inferences drawn

Social networks

Identifiers; information relating to Internet activity or other electronic network activity; audio, electronic, or visual information; information related to characteristics protected under California or federal law

If you are a minor under the age of 18 residing in the State of California, United States, You have additional rights under California law. You may request removal of any information or content you posted while under the age of 18. We cannot ensure that removal of information you provided to the Service will be complete or comprehensive (i.e., information posted to public groups and forums that may be accessed by non-users) but it will be complete and comprehensive on our part (i.e., user account information).

5. WHAT IS OUR STANCE ON THIRD-PARTY WEBSITES?

In Short: We are not responsible for the safety of any information that you share with third parties that we may link to or who advertise on our Services, but are not affiliated with, our Services.

The Services, [\[including our offer wall\]](#), may link to third-party websites, online services, or mobile applications and/or contain advertisements from third parties that are not affiliated with us and which may link to other websites, services, or applications. Accordingly, we do not make any guarantee regarding any such third parties, and we will not be liable for any loss or damage caused by the use of such third-party websites, services, or applications. The inclusion of a link towards a third-party website, service, or application does not imply an endorsement by us. We cannot guarantee the safety and privacy of data you provide to any third parties. Any data collected by third parties is not covered by this

privacy notice. We are not responsible for the content or privacy and security practices and policies of any third parties, including other websites, services, or applications that may be linked to or from the Services. You should review the policies of such third parties and contact them directly to respond to your questions.

7. Links to other websites

The Service may contain links to other websites not operated or controlled by OpenAI, including social media services ("Third Party Sites"). The information that you share with Third Party Sites will be governed by the specific privacy policies and terms of service of the Third Party Sites and not by this Privacy Policy. By providing these links we do not imply that we endorse or have reviewed these sites. Please contact the Third Party Sites directly for information on their privacy practices and policies.

6. DO WE USE COOKIES AND OTHER TRACKING TECHNOLOGIES?

***In Short:** We may use cookies and other tracking technologies to collect and store your information.*

We may use cookies and similar tracking technologies (like web beacons and pixels) to access or store information. Specific information about how we use such technologies and how you can refuse certain cookies is set out in our Cookie Notice: [\[Cookie Notice URL\]](#).

28. Cookies and Similar Technologies

We use cookies and similar tracking technologies to collect and use personal data about you, including to serve interest-based advertising. This section provides information about the types of cookies we use, their purpose, and how you can manage your cookie preferences.

Types of Cookies We Use

- ***Essential Cookies*:** These

11. ***Cookies and Tracking Technologies*:** Provide information about the use of cookies, web beacons, tracking pixels, and similar technologies, including the types of cookies used, their purpose, and how users can manage cookie preferences.

cookies

Cookies Policy

This Cookies Policy explains how our website uses cookies and similar tracking technologies. By accessing or using our website, you consent to the use of cookies as described in this policy.

What are Cookies?

Cookies are small text files that are placed on your computer or mobile device when you visit a website. They are widely used to make websites work more efficiently and to provide information to the owners of the site.

Types of Cookies We Use

- ***Essential Cookies***: These cookies are necessary for the website to function properly. They enable core functionalities such as security, network management, and accessibility.

- ***Analytical Cookies***: These cookies allow us to analyze how visitors use our website, so we can measure and improve its performance. We use Google Analytics and similar tools to collect information about website traffic and usage patterns.

- ***Functionality Cookies***: These cookies enable enhanced functionality and personalization, such as remembering your preferences or settings.

- ***Advertising Cookies***: These cookies are used to deliver advertisements that are relevant to you and your interests. They may be used by third-party advertisers to track your browsing activity across different websites.

Third-Party Cookies

We may also use third-party cookies provided by trusted partners for analytics, advertising, and other purposes. These cookies are subject to the respective privacy policies of the third-party providers.

Managing Cookies

You can control and/or delete cookies as you wish. Most web browsers allow you to manage cookies through their settings. You can also opt-out of certain cookies by using the opt-out tools provided by third-party advertisers.

Please note that disabling or blocking certain cookies may affect the functionality of our website.

7. HOW DO WE HANDLE YOUR SOCIAL LOGINS?

In Short: *If you choose to register or log in to our Services using a social media account, we may have access to certain information about you.*

Our Services offer you the ability to register and log in using your third-party social media account details (like your Facebook or Twitter logins). Where you choose to do this, we will receive certain profile information about you from your social media provider. The profile information we receive may vary depending on the social media provider concerned, but will often include your name, email address, friends list, and profile picture, as well as other information you choose to make public on such a social media platform. [\[If you log in using Facebook, we may also request access to other permissions related](#)

to your account, such as your friends, check-ins, and likes, and you may choose to grant or deny us access to each individual permission.]

We will use the information we receive only for the purposes that are described in this privacy notice or that are otherwise made clear to you on the relevant Services. Please note that we do not control, and are not responsible for, other uses of your personal information by your third-party social media provider. We recommend that you review their privacy notice to understand how they collect, use and share your personal information, and how you can set your privacy preferences on their sites and apps.

8. IS YOUR INFORMATION TRANSFERRED INTERNATIONALLY?

***In Short:** We may transfer, store, and process your information in countries other than your own.*

Our servers are located in [Country]. If you are accessing our Services from outside [Country], please be aware that your information may be transferred to, stored, and processed by us in our facilities and by those third parties with whom we may share your personal information (see "[WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?](#)" above), in [Country], and other countries.

If you are a resident in the European Economic Area (EEA), United Kingdom (UK), or Switzerland, then these countries may not necessarily have data protection laws or other similar laws as comprehensive as those in your country. However, we will take all necessary measures to protect your personal information in accordance with this privacy notice and applicable law.

European Commission's Standard Contractual Clauses:

We have implemented measures to protect your personal information, including by using the European Commission's Standard Contractual Clauses for transfers of personal information between our group companies and between us and our third-party providers. These clauses require all recipients to protect all personal information that they process originating from the EEA or UK in accordance with European data protection laws and regulations. Our Data Processing Agreements that include Standard Contractual Clauses are available here: [\[Standard Contractual Clauses URL\]](#). We have implemented similar appropriate safeguards with our third-party service providers and partners and further details can be provided upon request.

Binding Corporate Rules:

These include a set of Binding Corporate Rules ("BCRs") established and implemented by us. Our BCRs have been recognized by EEA and UK data protection authorities as providing an adequate level of

protection to the personal information we process internationally. You can find a copy of our BCRs here: [\[BCRs URL\]](#).

[\[EU-US\]](#) and [\[Swiss-US\]](#) Privacy Shield Framework[\[s\]](#)

We and the following entities and subsidiaries: [\[List of Entities/Subsidiaries\]](#) comply with the [\[EU-US\]](#) and [\[Swiss-US\]](#) Privacy Shield Framework[\[s\]](#) as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from [\[the European Union \(EU\)\]](#), [\[the UK\]](#), and [\[Switzerland\]](#) to the United States. Although Privacy Shield is no longer considered a valid transfer mechanism for the purposes of [\[EU\]](#) and [\[Swiss\]](#) data protection law, in light of the judgment of the Court of Justice of the European Union in Case C-311/18 and opinion of the Federal Data Protection and Information Commissioner of Switzerland dated 8 September 2020, we will continue to comply with the principles of the [\[EU-US\]](#) and [\[Swiss-US\]](#) Privacy Shield Framework[\[s\]](#). Learn more about the [Privacy Shield program](#). To view our certification, please visit [\[Privacy Shield Certification URL\]](#).

We adhere to and comply with the Privacy Shield Principles when processing personal information from [\[the EU\]](#), [\[UK\]](#), or [\[Switzerland\]](#). If we have received your personal information in the United States and subsequently transfer that information to a third party acting as our agent, and such third party agent processes your personal information in a manner inconsistent with the Privacy Shield Principles, we will remain liable unless we can prove we are not responsible for the event giving rise to the damage.

With respect to personal information received or transferred pursuant to the Privacy Shield Framework[\[s\]](#), we are subject to the investigatory and enforcement powers of the US Federal Trade Commission ("FTC"). In certain situations, we may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

If you have any questions or concerns relating to our Privacy Shield certification, please write to us at the contact details below. We commit to resolving any complaints or disputes about our collection and use of your personal information under the Privacy Shield. [\[However, if you have an unresolved complaint in connection with our certification, we commit to cooperating with the panel established by \[the EU data protection authorities \(DPAs\)\], \[the UK Information Commissioner\], and \[the Swiss Federal Data Protection and Information Commissioner\], as applicable, and to comply with the advice given by them in respect of the complaint. See the following \[list of EU DPAs\]\(#\). / However, if you have an unresolved complaint in connection with our certification, you may contact our independent dispute resolution provider based in the \[EU/United States\], \[Dispute Resolution Provider Name\]. Please visit \[Dispute Resolution Provider URL\] for more information or to file a complaint. These services are provided to you free of charge.\]](#)

In limited situations, [\[EU\]](#), [\[UK\]](#), and [\[Swiss\]](#) individuals may seek redress from the Privacy Shield Panel, a binding arbitration mechanism.

Please be sure to review the following sections of this privacy notice for additional details relevant to our participation in the [\[EU-US\]](#) and [\[Swiss-US\]](#) Privacy Shield:

- [WHAT INFORMATION DO WE COLLECT?](#) *To learn more about the types of personal data we collect.*
- [HOW DO WE PROCESS YOUR INFORMATION?](#) *To learn more about the purposes for which we collect and use personal information about you.*
- [WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?](#) *To learn more about the type or identity of third parties to which we disclose personal information, and the purposes for which we do so.*
- [WHAT ARE YOUR PRIVACY RIGHTS?](#) *To learn more about the right of individuals to access their personal data.*

9. HOW LONG DO WE KEEP YOUR INFORMATION?

In Short: *We keep your information for as long as necessary to fulfill the purposes outlined in this privacy notice unless otherwise required by law.*

We will only keep your personal information for as long as it is necessary for the purposes set out in this privacy notice, unless a longer retention period is required or permitted by law (such as tax, accounting, or other legal requirements). No purpose in this notice will require us keeping your personal information for longer than [\[the period of time in which users have an account with us / \[#\] months past the termination of the user's account / \[#\] months past the start of the idle period of the user's account / other\]](#).

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize such information, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

10. HOW DO WE KEEP YOUR INFORMATION SAFE?

In Short: *We aim to protect your personal information through a system of organizational and technical security measures.*

We have implemented appropriate and reasonable technical and organizational security measures designed to protect the security of any personal information we process. However, despite our

safeguards and efforts to secure your information, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security and improperly collect, access, steal, or modify your information. Although we will do our best to protect your personal information, transmission of personal information to and from our Services is at your own risk. You should only access the Services within a secure environment.

8. Security and retention

We implement commercially reasonable technical, administrative, and organizational measures to protect Personal Information both online and offline from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. However, no Internet or email transmission is ever fully secure or error free. In particular, email sent to or from us may not be secure. Therefore, you should take special care in deciding what information you send to us via the Service or email. In addition, we are not responsible for circumvention of any privacy settings or security measures contained on the Service, or third-party websites.

We'll retain your Personal Information for only as long as we need in order to provide our Service to you, or for other legitimate business purposes such as resolving disputes, safety and security reasons, or complying with our legal obligations. How long we retain Personal Information will depend on a number of factors, such as the amount, nature, and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure, our purpose for processing the information, and any legal requirements.

11. DO WE COLLECT INFORMATION FROM MINORS?

In Short: We do not knowingly collect data from or market to children under 18 years of age.

We do not knowingly solicit data from or market to children under 18 years of age. By using the Services, you represent that you are at least 18 or that you are the parent or guardian of such a minor and consent to such minor dependent's use of the Services. If we learn that personal information from users less than 18 years of age has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we may have collected from children under age 18, please contact us at [\[Email Address\]](#).

6. Children

Our Service is not directed to children under the age of 13. OpenAI does not knowingly collect Personal Information from children under the age of 13. If you have reason to believe that a child under the age of 13 has provided Personal Information to OpenAI through the Service, please email us at legal@openai.com. We will investigate any notification and if appropriate, delete the Personal Information from our systems. If you are 13 or older, but under 18, you must have permission from your parent or guardian to use our Services.

12. WHAT ARE YOUR PRIVACY RIGHTS?

In Short: *In some regions, such as the European Economic Area (EEA), United Kingdom (UK), Switzerland, and Canada, you have rights that allow you greater access to and control over your personal information. You may review, change, or terminate your account at any time.*

In some regions (like the EEA, UK, Switzerland, and Canada), you have certain rights under applicable data protection laws. These may include the right (i) to request access and obtain a copy of your personal information, (ii) to request rectification or erasure; (iii) to restrict the processing of your personal information; (iv) if applicable, to data portability; and (v) not to be subject to automated decision-making. In certain circumstances, you may also have the right to object to the processing of your personal information. You can make such a request by contacting us by using the contact details provided in the section "[HOW CAN YOU CONTACT US ABOUT THIS NOTICE?](#)" below.

We will consider and act upon any request in accordance with applicable data protection laws.

If you are located in the EEA or UK and you believe we are unlawfully processing your personal information, you also have the right to complain to your [Member State data protection authority](#) or [UK data protection authority](#).

If you are located in Switzerland, you may contact the [Federal Data Protection and Information Commissioner](#).

Withdrawing your consent: If we are relying on your consent to process your personal information, which may be express and/or implied consent depending on the applicable law, you have the right to withdraw your consent at any time. You can withdraw your consent at any time by contacting us by using the contact details provided in the section "[HOW CAN YOU CONTACT US ABOUT THIS NOTICE?](#)" below or updating your preferences.

However, please note that this will not affect the lawfulness of the processing before its withdrawal nor, when applicable law allows, will it affect the processing of your personal information conducted in reliance on lawful processing grounds other than consent.

Opting out of marketing and promotional communications: You can unsubscribe from our marketing and promotional communications at any time by clicking on the unsubscribe link in the emails that we send, replying "STOP" or "UNSUBSCRIBE" to the SMS messages that we send, [\[Other\]](#) or by contacting us using the details provided in the section "[HOW CAN YOU CONTACT US ABOUT THIS NOTICE?](#)" below. You will then be removed from the marketing lists – however, we may still communicate with you, for example to send you service-related messages that are necessary for the administration and use of your account, to respond to service requests, or for other non-marketing purposes.

Account Information

If you would at any time like to review or change the information in your account or terminate your account, you can:

- Log in to your account settings and update your user account.
- Contact us using the contact information provided.
- [\[Other\]](#)

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, we may retain some information in our files to prevent fraud, troubleshoot problems, assist with any investigations, enforce our legal terms and/or comply with applicable legal requirements.

Cookies and similar technologies: Most Web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and to reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features or services of our Services. You may also [opt out of interest-based advertising by advertisers](#) on our Services. For further information, please see our Cookie Notice: [\[Cookie Notice URL\]](#).

If you have questions or comments about your privacy rights, you may email us at [\[Email Address\]](#).

F. Your Privacy Rights

If you are a California resident, you have the following rights under applicable California law in relation to your personal information, subject to certain exceptions:

Right to Know. You have the right to, up to twice in a 12-month period, request what personal information we collect, use, disclose, and/or sell, as applicable.

Right to Delete. You have the right to request under certain circumstances the deletion of your personal information that is collected by us.

Right to Opt-Out of Sale or Sharing. You have the right to opt-out of the sale or sharing of your personal information by a business.

Right to Non-Discrimination. You have the right not to receive discriminatory treatment for the exercise of the privacy rights described above.

Right to Correct. You have the right to correct your information to exercise your privacy rights described above.

Any request you submit to us is subject to an identification and residency verification process ("Verifiable Consumer Request") as permitted by the CCPA. We will not fulfill your request unless you have provided sufficient information that enables us to reasonably verify that you are the consumer about whom we collected the personal information on. In order to verify you, you must provide us with your email address and your BeatStars username. These rights are also subject to various exclusions and exceptions under applicable laws.

You may also designate an authorized agent, in writing or through a power of attorney, to request to exercise the above rights on your behalf. The authorized agent may submit a request to exercise these rights by emailing the letter of authorization or power of attorney to .

We currently do not collect household data. If we receive a Right to Know or Right to Delete request submitted by all members of a household, we will individually respond to each request. We will not be able to comply with any request by a member of a household under the age of 13, as we do not collect personal information from any person under the age of 13.

We will respond to your request within forty-five (45) days after receipt of a Verifiable Consumer Request for a period covering twelve (12) months and for no more than twice in a twelve-month period. BeatStars reserves the right to extend the response time by an additional forty-five (45) days when reasonably necessary and provided consumer notification of the extension is made within the first forty-five (45) days.

You may exercise any of the rights described in this section by completing the online webform or by emailing us at .

G. Notice of Right to Opt-Out

We do not sell your personal information. If you wish to opt-out of our sharing of the limited data that is gathered when you visit our Site for purposes of targeted digital advertising, we encourage you to visit the and/or the Digital Advertising Alliance's for more information about opting out of seeing targeted digital advertisements. You may also visit these websites for more information on how you can opt back in to the sharing of data. Please note that BeatStars does not maintain this web tracking data in an identifiable manner. California-based users can opt out of performance, targeting, and social media cookies and SDKs by selecting the "Do Not Sell or Share My Personal Information" link in their cookie or SDK settings.

You can use these resources or other plugins to opt out of cookies through your browser:

Common browser settings:

We will continue to update our business practices as direct regulatory guidance becomes available. For more information on interest-based advertising, please visit our and .

4. Your rights

Depending on location, individuals may have certain statutory rights in relation to their Personal Information. For example, you may have the right to:

Access your Personal Information and information relating to how it is processed.

Delete your Personal Information from our records.

Rectify or update your Personal Information.

Transfer your Personal Information to a third party (right to data portability).

Restrict how we process your Personal Information.

Withdraw your consent—where we rely on consent as the legal basis for processing at any time.

Object to how we process your Personal Information.

Lodge a complaint with your local data protection authority.

You can exercise some of these rights through your OpenAI account. If you are unable to exercise your rights through your account, please submit your request through privacy.openai.com(opens in a new window) or to dsar@openai.com.

A note about accuracy: Services like ChatGPT generate responses by reading a user's request and, in response, predicting the words most likely to appear next. In some cases, the words most likely to appear next may not be the most factually accurate. For this reason, you should not rely on the factual accuracy of output from our models. If you notice that ChatGPT output contains factually inaccurate information about you and you would like us to correct the inaccuracy, you may submit a correction request through privacy.openai.com(opens in a new window) or to dsar@openai.com. Given the technical complexity of how our models work, we may not be able to correct the inaccuracy in every instance. In that case, you may request that we remove your Personal Information from ChatGPT's output by filling out this form(opens in a new window).

For information on how to exercise your rights with respect to data we have collected from the internet to train our models, please see this help center article(opens in a new window).

21. Data Subject Requests

We are committed to responding to your requests to exercise your privacy rights in a timely manner. To make a request, please contact us using the details provided in the "Contact Us" section. We may need to verify your identity before processing your request.

- ***Verification Process***: To verify your identity, we may request information that matches the personal data we have on file for you. This is to ensure that your data is protected and only accessed by you or your authorized representative.

20. ***Data Subject Requests***: Explain how users can exercise their privacy rights, such as accessing, correcting, or deleting their personal information, and provide instructions on how to submit such requests.

53. ***Data Subject Rights Procedures***: Detail the procedures and timelines for responding to data subject rights requests, including verification of identity and communication methods.

77. ***Data Subject Access Requests (DSARs)***: Explain the process for handling data subject access requests, including the timeframe for responding, verifying the requester's identity, and providing requested information.

78. ***Data Subject Rectification Requests***: Outline procedures for correcting inaccurate or incomplete personal data upon request from data subjects, including how rectifications are communicated to third parties, if applicable.

79. ***Data Subject Erasure Requests (Right to be Forgotten)***: Detail the process for honoring data subjects' requests to delete their personal data, including any exceptions or limitations under applicable law.

80. ***Data Subject Objection Requests***: Explain how data subjects can object to certain processing activities (e.g., direct marketing) and the steps taken to address objections, including ceasing processing or providing opt-out mechanisms.

82. ***Data Subject Consent Withdrawal***: Inform users of their right to withdraw consent to processing activities and the implications of withdrawing consent, such as limitations on service availability or features.

83. ***Data Subject Complaint Escalation Procedures***: Specify escalation procedures for handling unresolved data subject complaints, including contact information for relevant supervisory authorities or dispute resolution mechanisms.

85. ***Data Subject Rights Training for Staff***: Provide training to staff members responsible for handling data subject requests to ensure they understand their obligations and responsibilities under applicable privacy laws.

86. ***Data Subject Consent Revocation Mechanisms***: Implement mechanisms for data subjects to easily revoke consent to processing activities, such as through user account settings or dedicated opt-out mechanisms.

87. ***Data Subject Consent Documentation***: Maintain documentation of user consent, including the version of the privacy policy at the time of consent, the purpose of processing, and any specific consent preferences expressed by the user.

88. ***Data Subject Consent Confirmation***: Provide confirmation to data subjects upon the successful submission of consent preferences, including a summary of the processing activities covered by the consent and the effective date of consent.

89. ***Data Subject Consent Renewal Notices***: Periodically remind data subjects of their consent preferences and provide opportunities to review and update their consent settings, especially in cases where consent expiration dates are specified.

90. ***Data Subject Consent Withdrawal Confirmation***: Confirm the successful withdrawal of consent to data subjects and provide guidance on any additional steps they may need to take to ensure the cessation of processing activities covered by the revoked consent.

91. ***Data Subject Consent Granularity***: Offer granular consent options to data subjects, allowing them to choose specific processing activities or categories of personal data they consent to, rather than providing blanket consent.

92. ***Data Subject Consent Preferences Dashboard***: Provide data subjects with access to a consent preferences dashboard or control panel where they can manage their consent settings, view consent history, and exercise consent-related rights.

93. ***Data Subject Consent Recipients***: Disclose the recipients or categories of recipients with whom data subjects' consented personal data may be shared, along with the purposes for which the data will be shared.

94. ***Data Subject Consent Duration***: Specify the duration of data subjects' consent preferences, including any expiration dates or conditions under which consent may be automatically renewed or revoked.

95. ***Data Subject Consent Verification***: Implement mechanisms to verify data subjects' consent preferences, such as confirmation emails, two-factor authentication, or captcha tests, to prevent unauthorized changes to consent settings.

96. ***Data Subject Consent Preferences History***: Maintain a historical record of data subjects' consent preferences, including the date and time of consent changes, the specific preferences selected, and the version of the privacy policy at the time of consent.

97. ***Data Subject Consent Transparency***: Provide transparency regarding the scope and implications of data subjects' consent preferences, including explanations of processing activities covered by the consent and any associated risks or benefits.

98. ***Data Subject Consent Acknowledgment***: Require data subjects to acknowledge their understanding of the implications of providing or withholding consent to processing activities, such as through checkbox acknowledgments or digital signatures.

99. ***Data Subject Consent Revalidation***: Prompt data subjects to revalidate their consent preferences periodically

4. ***Data Subject Rights***: Inform users of their rights regarding their personal information, such as the right to access, rectify, or delete their data, and provide instructions on how to exercise those rights.

13. CONTROLS FOR DO-NOT-TRACK FEATURES

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. At this stage no uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this privacy notice.

14. DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?

In Short: *If you are a resident of California, Colorado, Connecticut, Utah, or Virginia, you are granted specific rights regarding access to your personal information.*

What categories of personal information do we collect?

We have collected the following categories of personal information in the past twelve (12) months:

Category	Examples	Collected
A. Identifiers	Contact details, such as real name, alias, postal address, telephone or mobile contact number, unique personal identifier, online identifier, Internet Protocol address, email address, and account name	[YES/NO]
B. Personal information as defined in the California Customer Records statute	Name, contact information, education, employment, employment history, and financial information	[YES/NO]
C. Protected classification characteristics under state or federal law	Gender and date of birth	[YES/NO]
D. Commercial information	Transaction information, purchase history, financial details, and payment information	[YES/NO]

E. Biometric information	Fingerprints and voiceprints	[YES/NO]
F. Internet or other similar network activity	Browsing history, search history, online behavior, interest data, and interactions with our and other websites, applications, systems, and advertisements	[YES/NO]
G. Geolocation data	Device location	[YES/NO]
H. Audio, electronic, visual, thermal, olfactory, or similar information	Images and audio, video or call recordings created in connection with our business activities	[YES/NO]
I. Professional or employment-related information	Business contact details in order to provide you our Services at a business level or job title, work history, and professional qualifications if you apply for a job with us	[YES/NO]
J. Education information	Student records and directory information	[YES/NO]
K. Inferences drawn from collected personal information	Inferences drawn from any of the collected personal information listed above to create a profile or summary about, for example, an individual's preferences and characteristics	[YES/NO]
L. Sensitive personal information	Account login information, drivers' licenses, health data, precise geolocation, racial or ethnic origin, religious or philosophical beliefs, and sex life or sexual orientation	[YES/NO]

We will use and retain the collected personal information as needed to provide the Services or for:

- Category A - [\[Retention Period\]](#)
- Category B - [\[Retention Period\]](#)
- Category C - [\[Retention Period\]](#)

- Category D - [\[Retention Period\]](#)
- Category E - [\[Retention Period\]](#)
- Category F - [\[Retention Period\]](#)
- Category G - [\[Retention Period\]](#)
- Category H - [\[Retention Period\]](#)
- Category I - [\[Retention Period\]](#)
- Category J - [\[Retention Period\]](#)
- Category K - [\[Retention Period\]](#)
- Category L - [\[Retention Period\]](#)

Category L information may be used, or disclosed to a service provider or contractor, for additional, specified purposes. You have the right to limit the use or disclosure of your sensitive personal information.

We may also collect other personal information outside of these categories through instances where you interact with us in person, online, or by phone or mail in the context of:

- Receiving help through our customer support channels;
- Participation in customer surveys or contests; and
- Facilitation in the delivery of our Services and to respond to your inquiries.

How do we use and share your personal information?

Learn about how we use your personal information in the section, "[HOW CAN YOU CONTACT US ABOUT THIS NOTICE?](#)"

We collect and share your personal information through:

- Targeting cookies/Marketing cookies
- Social media cookies
- Beacons/Pixels/Tags
- Click redirects: [\[Click Redirects\]](#)
- Social media plugins: [\[Social Media Plugins\]](#). We use social media features, such as a "Like" button, and widgets, such as a "Share" button in our Services. Such features may process your Internet Protocol (IP) address and track which page you are visiting on our website. We may place a cookie to enable the feature to work correctly. If you are logged in on a certain social media platform and you interact with a widget or button belonging to that social media platform, this information may be recorded to your profile of such social media platform. To avoid this, you should log out from that social media platform before accessing or using the Services. Social media features and widgets may be hosted by a third party or hosted directly on our Services.

Your interactions with these features are governed by the privacy notices of the companies that provide them. By clicking on one of these buttons, you agree to the use of this plugin and consequently the transfer of personal information to the corresponding social media service. We have no control over the essence and extent of these transmitted data or their additional processing.

- [\[Other\]](#)

Will your information be shared with anyone else?

We may disclose your personal information with our service providers pursuant to a written contract between us and each service provider. Learn more about who we disclose personal information to in the section, "[WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?](#)"

We may use your personal information for our own business purposes, such as for undertaking internal research for technological development and demonstration. This is not considered to be "selling" of your personal information.

We have disclosed the following categories of personal information to third parties for a business or commercial purpose in the preceding twelve (12) months:

- Category A. Identifiers
- Category B. Personal information, as defined in the California Customer Records law
- Category C. Characteristics of protected classifications under state or federal law
- Category D. Commercial information
- Category E. Biometric information
- Category F. Internet or other electronic network activity information
- Category G. Geolocation data
- Category H. Audio, electronic, visual, and similar information
- Category I. Professional or employment-related information
- Category J. Education information
- Category K. Inferences drawn from collected personal information
- Category L. Sensitive personal information

The categories of third parties to whom we disclosed personal information for a business or commercial purpose can be found under "[WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?](#)"

We have not sold or shared any personal information to third parties for a business or commercial purpose in the preceding twelve (12) months. / We have sold or shared the following categories of personal information to third parties in the preceding twelve (12) months:

- Category A. Identifiers
- Category B. Personal information, as defined in the California Customer Records law
- Category C. Characteristics of protected classifications under state or federal law
- Category D. Commercial information
- Category E. Biometric information
- Category F. Internet or other electronic network activity information
- Category G. Geolocation data
- Category H. Audio, electronic, visual, and similar information
- Category I. Professional or employment-related information
- Category J. Education information
- Category K. Inferences drawn from collected personal information
- Category L. Sensitive personal information

The categories of third parties to whom we sold personal information are:

- Ad Networks
- Affiliate Marketing Programs
- Data Analytics Services
- Retargeting Platforms
- Social Networks
- User Account Registration & Authentication Services
- [Other]

The categories of third parties to whom we shared personal information with are:

- Ad Networks
- Affiliate Marketing Programs
- Data Analytics Services
- Retargeting Platforms
- Social Networks
- User Account Registration & Authentication Services
- [Other]]

California Residents

California Civil Code Section 1798.83, also known as the "Shine The Light" law, permits our users who are California residents to request and obtain from us, once a year and free of charge, information about categories of personal information (if any) we disclosed to third parties for direct marketing purposes and the names and addresses of all third parties with which we shared personal information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to us using the contact information provided below.

If you are under 18 years of age, reside in California, and have a registered account with Services, you have the right to request removal of unwanted data that you publicly post on the Services. To request removal of such data, please contact us using the contact information provided below and include the email address associated with your account and a statement that you reside in California. We will make sure the data is not publicly displayed on the Services, but please be aware that the data may not be completely or comprehensively removed from all our systems (e.g., backups, etc.).

CCPA Privacy Notice

This section applies only to California residents. Under the California Consumer Privacy Act (CCPA), you have the rights listed below.

The California Code of Regulations defines a "resident" as:

- (1) every individual who is in the State of California for other than a temporary or transitory purpose and
- (2) every individual who is domiciled in the State of California who is outside the State of California for a temporary or transitory purpose

All other individuals are defined as "non-residents."

If this definition of "resident" applies to you, we must adhere to certain rights and obligations regarding your personal information.

Your rights with respect to your personal data

Right to request deletion of the data – Request to delete

You can ask for the deletion of your personal information. If you ask us to delete your personal information, we will respect your request and delete your personal information, subject to certain

exceptions provided by law, such as (but not limited to) the exercise by another consumer of his or her right to free speech, our compliance requirements resulting from a legal ob`

Depending on the circumstances, you have a right to know:

- whether we collect and use your personal information;
- the categories of personal information that we collect;
- the purposes for which the collected personal information is used;
- whether we sell or share your personal information to third parties;
- the categories of personal information that we sold, shared, or disclosed for a business purpose;
- the categories of third parties to whom the personal information was sold, shared, or disclosed for a business purpose;
- the business or commercial purpose for collecting, sharing, or selling personal information; and
- the specific pieces of personal information we collected about you.

In accordance with applicable law, we are not obligated to provide or delete consumer information that is de-identified in response to a consumer request or to re-identify individual data to verify a consumer request.

Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights

We will not discriminate against you if you exercise your privacy rights.

Right to Limit Use and Disclosure of Sensitive Personal Information

[We do not process consumer's sensitive personal information. / If the business collects any of the following:

- social security information, drivers' licenses, state ID cards, passport numbers
- account login information
- credit card numbers, financial account information, or credentials allowing access to such accounts
- precise geolocation
- racial or ethnic origin, religious or philosophical beliefs, union membership
- the contents of email and text, unless the business is the intended recipient of the communication
- genetic data, biometric data, and health data
- data concerning sexual orientation and sex life

you have the right to direct that business to limit its use of your sensitive personal information to that use which is necessary to perform the Services.

Once a business receives your request, they are no longer allowed to use or disclose your sensitive personal information for any other purpose unless you provide consent for the use or disclosure of sensitive personal information for additional purposes.

Please note that sensitive personal Information that is collected or processed without the purpose of inferring characteristics about a consumer is not covered by this right, as well as the publicly available information.

To exercise your right to limit use and disclosure of sensitive personal Information, please email [Email Address] or visit: [DSAR Form URL].]

Verification process

Upon receiving your request, we will need to verify your identity to determine you are the same person about whom we have the information in our system. These verification efforts require us to ask you to provide information so that we can match it with information you have previously provided us. For instance, depending on the type of request you submit, we may ask you to provide certain information so that we can match the information you provide with the information we already have on file, or we may contact you through a communication method (e.g., phone or email) that you have previously provided to us. We may also use other verification methods as the circumstances dictate.

We will only use personal information provided in your request to verify your identity or authority to make the request. To the extent possible, we will avoid requesting additional information from you for the purposes of verification. However, if we cannot verify your identity from the information already maintained by us, we may request that you provide additional information for the purposes of verifying your identity and for security or fraud-prevention purposes. We will delete such additionally provided information as soon as we finish verifying you.

Other privacy rights

- You may object to the processing of your personal information.
- You may request correction of your personal data if it is incorrect or no longer relevant, or ask to restrict the processing of the information.
- You can designate an authorized agent to make a request under the CCPA on your behalf. We may deny a request from an authorized agent that does not submit proof that they have been validly authorized to act on your behalf in accordance with the CCPA.
- [You may request to opt out from future selling or sharing of your personal information to third parties. Upon receiving an opt-out request, we will act upon the request as soon as feasibly possible, but no later than fifteen (15) days from the date of the request submission.]

[\[You can opt out from the selling or sharing of your personal information by disabling cookies in Cookie Preference Settings and clicking on the Do Not Sell or Share My Personal Information link on our homepage.\]](#)

Do not sell my personal information

Effective date: 06/06/2022

BeatStars Inc. ("BeatStars", "us", "we", or "our") is 100% committed to our customers and community, which is why we want to take the time to explain exactly what the "Do Not Sell My Personal Information" link on BeatStars webpages and apps means. The purpose of this article is to explain (1) why BeatStars' webpages and apps contain the "Do Not Sell" link, (2) what it means to "sell" "personal information," as those terms are defined under California law (3) that BeatStars does not sell personal information that directly identifies you, even under the California definition of "sale," (4) what happens if you tell BeatStars not to "sell" your personal information, (5) how BeatStars implements your choice to block it from "selling" your personal information, and (6) how BeatStars maintains your "Do Not Sell" Choice.

Why Does BeatStars Provide the "Do Not Sell" Link?

BeatStars provides the "Do Not Sell" link to comply with the California Consumer Privacy Act (CCPA), California Civil Code Section 1798.100 et seq., effective January 1, 2020. The CCPA is a new data protection law that provides California residents with certain choices about their data, including the ability to tell companies not to "sell" their personal information. The link is there to inform you of this choice. Although the CCPA only gives California residents the right to make these requests, we allow non-California residents with the same choices about their personal information. Please see our [for more information](#).

What Does it Mean to "Sell" "Personal Information" Under the CCPA?

The CCPA broadens the definition of "sale" and "personal information" beyond how you might commonly interpret those terms.

Under the CCPA, "personal information" includes information that is not necessarily directly tied to an individual's identity but may be associated with a device. This includes identifiers such as IP addresses, web cookies, web beacons, and mobile AdIDs. In many cases, this type of information is not associated with you, but they are unique identifiers that could be. Similarly, the term "sell" is defined to include not just selling in exchange for money, but also sharing or transferring personal information (including information that does not directly identify an individual as described above) in exchange for anything of value, which is not limited to the exchange of money. Certain things are not considered "sales," including when (1) personal information is shared with a service provider that is contractually prohibited from using the personal information for any purpose beyond the service specifically requested ("service provider exception"), or (2) when the consumer has directed a company to disclose the personal information ("consumer directed exception").

Does BeatStars "Sell" my Personal Information?

BeatStars does not sell information that directly identifies you, like your name, address, social security number, banking information, or phone records. In fact, we do not even share that type of information except with service providers who can use the information solely to provide a service on our behalf, when a consumer directs us to share the information, or in the limited additional circumstances outlined in our [\(such as for fraud prevention purposes or where we are legally required to share the information\)](#).

However, the CCPA's broad definitions of "sale" and "personal information" may deem the common flow of information in the digital analytics and advertising ecosystem to be a sale. Like most companies that operate commercial websites and apps, BeatStars utilizes online analytics to measure the ways users engage with our websites and apps. These analytics, in turn, inform how we perform online advertising. In order to provide these analytics and facilitate online advertising, BeatStars uses third-parties that collect device identifiers and place tags, cookies, beacons, and similar tracking mechanisms on our websites/apps and on third-party websites/apps. For instance, we may request that a third-party facilitate the placement of BeatStars ads on a particular website after a consumer has previously visited BeatStars. The third-parties we use for these

purposes generally do this by placing a cookie on a user's browser so it can identify that the same browser visited other websites. Similarly, where our webpages or apps provide space for advertisements, these third-parties may use identifiers such as cookies for websites, or the device's mobile AdID for apps, to facilitate real-time bidding by advertisers.

Where we can reasonably ensure via contract that the third-parties described above can and will use a device identifier solely to provide the specific service we have requested, and will not use or share the data for other purposes, we will not deem that sharing a "sale." In most cases, we've determined that our data analytics providers that measure the ways users engage with our websites and apps meet this standard and, accordingly, we will not block the sharing of an identifier with those entities even when you choose to opt-out through the "Do Not Sell" link.

In some cases, though, BeatStars does not ultimately control how such identifiers are used by some third-parties (particularly in some cases in the online advertising ecosystem), and so we can't determine that all sharing with third-parties in these cases fall within the service provider exception under the law.

What Happens when I Tell BeatStars not to "Sell" my Personal Information?

When a user of our websites/apps makes the "Do Not Sell" choice, we will attempt to block further sharing of the covered identifiers with the third-parties we engage on those digital properties or any other entity that does not fall within the service provider exception or the consumer directed exception.

How Does BeatStars Implement my Choice to Block it from "Selling" my Personal Information?

If you wish to opt-out of our sharing of the limited data that is gathered when you visit our Site for purposes of targeted digital advertising, we encourage you to visit the , the or the for more information about opting out of seeing targeted digital advertisements. Similarly, you can learn about your options to opt-out of mobile app tracking by certain advertising networks through your device settings.

You may also visit these websites for more information on how you can opt back into the sharing of data.

You can also opt out of interest-based advertising with some of the service providers we use, such as Google .

If you would like to exercise any of these rights, please contact us by emailing us at .

How Does BeatStars Maintain my "Do Not Sell" Choice?

If you choose to sign in and set a "Do Not Sell" setting tied to your account, we will attempt to identify and honor that setting on the BeatStars app or website. Please note that that setting may not work if your browser does not accept cookies or if you later delete cookies or delete data on your app.

Ad choices settings and options will vary depending on your browser and device settings, and this is not an exhaustive list. Please note that your opt-out choices will only apply to the specific browser or device from which you opt out. Please explore your device and browser settings to better understand your choices.

Connected devices (such as tablets, connected TVs, and other devices) may also use an advertising ID or other methods to identify you or serve you interest-based advertising. In some cases, you can disable tracking by selecting options like "limit ad tracking" or disabling options like "interest-based advertising" in your connected device's settings. These options will vary by device and we do not control the policies or practices of third parties' providing these devices. BeatStars is not responsible for tracking on connected devices or our business partners' services and may not have visibility on choices you may have made with respect to tracking on connected devices or our business partners' services.

For information on how to control your choices on those devices, you should contact those third parties directly to learn more about their privacy practices and any data they may collect and share or sell to third parties.

For more information about BeatStars' privacy practices and our approach to the CCPA, please see our .

To exercise these rights, you can contact us by visiting [\[DSAR Form URL\]](#), by email at [\[Email Address\]](#), by calling toll-free at [\[Phone Number\]](#), by visiting [\[Contact Form URL\]](#), or by referring to the contact details at the bottom of this document. If you have a complaint about how we handle your data, we would like to hear from you.

Financial Incentives

"Financial incentive" means a program, benefit, or other offering, including payments to consumers as compensation, for the disclosure, deletion, sharing, or sale of personal information.

The law permits financial incentives or a price or service difference if it is reasonably related to the value of the consumer's data. A business must be able to explain how the financial incentive or price or service difference is reasonably related to the value of the consumer's data. The explanation must include:

- a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and
- a description of the method the business used to calculate the value of the consumer's data.

We may decide to offer a financial incentive (e.g., price or service difference) in exchange for the retention, or sale or sharing of a consumer's personal information.

If we decide to offer a financial incentive, we will notify you of such financial incentive and explain the price difference, as well as material terms of the financial incentive or price of service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference.

If you choose to participate in the financial incentive you can withdraw from the financial incentive at any time by emailing us at [\[Email Address\]](#), by calling us toll-free at [\[Phone Number\]](#), by visiting [\[Contact Form URL\]](#), or by referring to the contact details at the bottom of this document.

Metrics

Our metrics for all CCPA requests received for the previous calendar year can be found here: [\[Metrics URL\]](#).

Colorado Residents

This section applies only to Colorado residents. Under the Colorado Privacy Act (CPA), you have the rights listed below. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by law.

- Right to be informed whether or not we are processing your personal data
- Right to access your personal data
- Right to correct inaccuracies in your personal data
- Right to request deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to opt out of the processing of your personal data if it is used for targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects (“profiling”)

[\[We sell personal data to third parties or process personal data for targeted advertising. You can opt out from the selling of your personal data, targeted advertising, or profiling by disabling cookies in Cookie Preference Settings.\]](#) To submit a request to exercise these rights described above, please email [\[Email Address\]](#) or visit [\[DSAR Form URL\]](#).

If we decline to take action regarding your request and you wish to appeal our decision, please email us at [\[Email Address\]](#). Within forty-five (45) days of receipt of an appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions.

Connecticut Residents

This section applies only to Connecticut residents. Under the Connecticut Data Privacy Act (CTDPA), you have the rights listed below. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by law.

- Right to be informed whether or not we are processing your personal data
- Right to access your personal data
- Right to correct inaccuracies in your personal data
- Right to request deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to opt out of the processing of your personal data if it is used for targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects (“profiling”)

[\[We sell personal data to third parties or process personal data for targeted advertising. You can opt out from the selling of your personal data, targeted advertising, or profiling by disabling cookies in Cookie Preference Settings.\]](#) To submit a request to exercise these rights described above, please email [\[Email Address\]](#) or visit [\[DSAR Form URL\]](#).

If we decline to take action regarding your request and you wish to appeal our decision, please email us at [\[Email Address\]](#). Within sixty (60) days of receipt of an appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions.

Utah Residents

This section applies only to Utah residents. Under the Utah Consumer Privacy Act (UCPA), you have the rights listed below. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by law.

- Right to be informed whether or not we are processing your personal data
- Right to access your personal data
- Right to request deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to opt out of the processing of your personal data if it is used for targeted advertising or the sale of personal data

[\[We sell personal data to third parties or process personal data for targeted advertising. You can opt out from the selling of your personal data, targeted advertising, or profiling by disabling cookies in Cookie Preference Settings.\]](#) To submit a request to exercise these rights described above, please email [\[Email Address\]](#) or visit [\[DSAR Form URL\]](#).

Virginia Residents

Under the Virginia Consumer Data Protection Act (VCDPA):

"Consumer" means a natural person who is a resident of the Commonwealth acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.

"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include de-identified data or publicly available information.

"Sale of personal data" means the exchange of personal data for monetary consideration.

If this definition of "consumer" applies to you, we must adhere to certain rights and obligations regarding your personal data.

Your rights with respect to your personal data

- Right to be informed whether or not we are processing your personal data
- Right to access your personal data
- Right to correct inaccuracies in your personal data
- Right to request deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to opt out of the processing of your personal data if it is used for targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects ("profiling")

[We sell personal data to third parties or process personal data for targeted advertising. Please see the following section to find out how you can opt out from further selling or sharing of your personal data for targeted advertising or profiling purposes.]

Exercise your rights provided under the Virginia VCDPA

[You can opt out from the selling of your personal data, targeted advertising, or profiling by disabling cookies in Cookie Preference Settings.]

You may contact us by email at [Email Address] or visit [Contact Form URL].

If you are using an authorized agent to exercise your rights, we may deny a request if the authorized agent does not submit proof that they have been validly authorized to act on your behalf.

Verification process

We may request that you provide additional information reasonably necessary to verify you and your consumer's request. If you submit the request through an authorized agent, we may need to collect additional information to verify your identity before processing your request.

Upon receiving your request, we will respond without undue delay, but in all cases, within forty-five (45) days of receipt. The response period may be extended once by forty-five (45) additional days when reasonably necessary. We will inform you of any such extension within the initial 45-day response period, together with the reason for the extension.

Right to appeal

If we decline to take action regarding your request, we will inform you of our decision and reasoning behind it. If you wish to appeal our decision, please email us at [\[Email Address\]](#). Within sixty (60) days of receipt of an appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If your appeal is denied, you may contact the [Attorney General to submit a complaint](#).

15. DO OTHER REGIONS HAVE SPECIFIC PRIVACY RIGHTS?

9. International users

By using our Service, you understand and acknowledge that your Personal Information will be processed and stored in our facilities and servers in the United States and may be disclosed to our service providers and affiliates in other jurisdictions.

Legal basis for processing. Our legal bases for processing your Personal Information include:

Performance of a contract with you when we provide and maintain our Services. When we process Account Information, Content, and Technical Information solely to provide our Services to you, this information is necessary to be able to provide our Services. If you do not provide this information, we may not be able to provide our Services to you.

Our legitimate interests in protecting our Services from abuse, fraud, or security risks, or in developing, improving, or promoting our Services, including when we train our models. This may include the processing of Account Information, Content, Social Information, and Technical Information. Read our instructions([opens in a new window](#)) on how you can opt out of our use of your information to train our models.

Your consent when we ask for your consent to process your Personal Information for a specific purpose that we communicate to you. You have the right to withdraw your consent at any time.

Compliance with our legal obligations when we use your Personal Information to comply with applicable law or when we protect our or our affiliates', users', or third parties' rights, safety, and property.

Data transfers. Where required, we will use appropriate safeguards for transferring Personal Information outside of certain countries. We will only transfer Personal Information pursuant to a legally valid transfer mechanism.

Data protection officer. You can contact our data protection officer at privacy@openai.com in matters related to Personal Information processing.

In Short: You may have additional rights based on the country you reside in.

Australia and New Zealand

We collect and process your personal information under the obligations and conditions set by Australia's Privacy Act 1988 and New Zealand's Privacy Act 2020 (Privacy Act).

This privacy notice satisfies the notice requirements defined in both Privacy Acts, in particular: what personal information we collect from you, from which sources, for which purposes, and other recipients of your personal information.

If you do not wish to provide the personal information necessary to fulfill their applicable purpose, it may affect our ability to provide our services, in particular:

- offer you the products or services that you want
- manage your account with us
- respond to or help with your requests
- confirm your identity and protect your account

At any time, you have the right to request access to or correction of your personal information. You can make such a request by contacting us by using the contact details provided in the section "[HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?](#)"

If you believe we are unlawfully processing your personal information, you have the right to submit a complaint about a breach of the Australian Privacy Principles to the [Office of the Australian Information Commissioner](#) and for a breach of New Zealand's Privacy Principles to the [Office of New Zealand Privacy Commissioner](#).

Republic of South Africa

At any time, you have the right to request access to or correction of your personal information. You can make such a request by contacting us by using the contact details provided in the section "[HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?](#)"

If you are unsatisfied with the manner in which we address any complaint with regard to our processing of personal information, you can contact the office of the regulator, the details of which are:

[The Information Regulator \(South Africa\)](#)

General enquiries: enquiries@inforegulator.org.za

Complaints (complete POPIA/PAIA form 5): PAIAComplaints@inforegulator.org.za & POPIAComplaints@inforegulator.org.za

16. DO WE MAKE UPDATES TO THIS NOTICE?

***In Short:** Yes, we will update this notice as necessary to stay compliant with relevant laws.*

We may update this privacy notice from time to time. The updated version will be indicated by an updated "Revised" date and the updated version will be effective as soon as it is accessible. If we make material changes to this privacy notice, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this privacy notice frequently to be informed of how we are protecting your information.

10. Changes to the privacy policy

We may update this Privacy Policy from time to time. When we do, we will post an updated version on this page, unless another type of notice is required by applicable law.

17. HOW CAN YOU CONTACT US ABOUT THIS NOTICE?

H. How To Contact Us

If you have any questions about this Privacy Policy or our privacy practices, please contact us by completing the online webform or by emailing us at .

I. CALIFORNIA "SHINE THE LIGHT" LAW

California residents additionally have the right to request information regarding third parties to whom BeatStars has disclosed certain categories of personal information during the preceding year for the third parties' direct marketing purposes under California's "Shine the Light" law (Cal. Civ. Code §1798.83). Personal information under this California law means "any information that when it was disclosed identified, described, or was able to be associated with an individual." We do not disclose this type of personal information to third parties for their own purposes and we permit you to opt-out of any disclosures of non-identifiable personal information. However, if you are a California resident and would like to inquire further, please email .

11. How to contact us

Please contact support(opens in a new window) if you have any questions or concerns not already addressed in this Privacy Policy.

If you have questions or comments about this notice, you may contact our Data Protection Officer (DPO), [DPO Name], by email at [Email Address], by phone at [Phone Number], or by post to:

[Company Name]

[DPO Name]

[Street Address]

[City, State ZIP Code]

[Country]

If you are a resident in the European Economic Area or Switzerland, we are the "data controller" of your personal information. We have appointed [EEA Representative Name] to be our representative in the EEA

and Switzerland. You can contact them directly regarding our processing of your information, by email at [\[Email Address\]](#), by visiting [\[EEA Representative URL\]](#), by phone at [\[Phone Number\]](#), or by post to:

[\[Street Address\]](#)

[\[City, State ZIP Code\]](#)

[\[Country\]](#)

Swiss Representative

[\[Swiss Representative Name\]](#)

[\[Street Address\]](#)

[\[City, State ZIP Code\]](#)

[\[Country\]](#)

Phone: [\[Phone Number\]](#)

Fax: [\[Fax Number\]](#)

[\[Swiss Representative URL\]](#)

If you are a resident in the United Kingdom, we are the "data controller" of your personal information. We have appointed [\[UK Representative Name\]](#) to be our representative in the UK. You can contact them directly regarding our processing of your information, by email at [\[Email Address\]](#), by visiting [\[UK Representative URL\]](#), by phone at [\[Phone Number\]](#), or by post to:

[\[Street Address\]](#)

[\[City, State ZIP Code\]](#)

[\[Country\]](#)

If you have any further questions or comments, you may also contact us by post at the following corporate address:

[\[Company Name\]](#)

[\[Street Address\]](#)

[\[City, State ZIP Code\]](#)

[\[Country\]](#)

Phone: [\[Phone Number\]](#)

Fax: [\[Fax Number\]](#)

18. HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?

Based on the applicable laws of your country, you may have the right to request access to the personal information we collect from you, change that information, or delete it. To request to review, update, or delete your personal information, please visit: [\[DSAR Form URL\]](#).

SOUND SAUCE

Privacy Policy

1. INTRO

- a. LAST UPDATED**
- b. PREAMBLE**
- c. DEFINITIONS**
- d. SUMMERY**
- e. CATALOG**

2. LEGAL BASIS

3. DATA WE COLLECT

- a. GEOLOCATION**

4. HOW WE USE DATA

- a. DATA USAGE FOR MARKETING AND ADVERTISING**
- b. AUTOMATED DECISION MAKING**

5. HOW WE STORE DATA

- a. DATA RETENTION**
- b. CHILDREN-MINOR'S DATA**

6. HOW WE SECURE DATA, SECURITY MEASURES AND GOVERNANCE

- a. SECURE - MEASURES**
- b. GOVERNANCE**

7. COOKIES

8. SENSITIVE - PERSONAL DATA AND INFORMATION

9. INTERNATIONAL - CROSS BORDER DATA TRANSFER

10. DATA SHARING

11. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

12. THIRD PARTIES

13. AUTOMATED DATA PROCESSING

14. YOUR RIGHTS

- a. DO NOT TRACK**
- b. OPT OUT MECHANISMS**

[illegible]

15.COMPLAINTS - NOTICES

16. GOVERNING LAW

17. RESIDENTS OF

a. (COUNTRIES) (GDPR-UK-CCPR-EGYPT-KSA-UAE-JORDAN-MOROCCO)

b. RESIDENTS OF OTHER COUNTRIES

18.DISCLOSURE OF INFORMATION

19. UPDATES TO PRIVACY POLICY

20. CONTACT US