

Viber United States Regional Privacy Notice

Last Updated: March 23, 2026

This United States Regional Privacy Notice (“**U.S. Notice**”) is a supplement to the Viber [Privacy Policy](#) and applies to United States residents including residents of California who are governed by the California Consumer Privacy Act of 2018, as amended and supplemented by any implementing regulations (“**CCPA**”). As of the date of this U.S. Notice, it supersedes both the prior CCPA Notice and the prior version of this U.S. Notice. Capitalized terms used but not defined herein shall have the same meaning as provided under the [Viber Terms of Service](#) or the [Viber Privacy Policy](#). This U.S. Notice details the categories of Personal Data (as the term is defined below) we collect, the type of source, the purposes of use, whether your Personal Data is sold or shared, the categories of recipients to whom we disclose your Personal Data, and the retention period. It also describes your privacy rights and how to exercise them under the various U.S. state comprehensive privacy laws and other federal and state laws, as may be applicable (all collectively shall be defined as “**U.S. Privacy Laws**”).

Table of Contents

- [1. Personal Data and Sensitive Data](#)
- [2. Categories of Personal Data or Sensitive Data We Collect](#)
- [3. Categories of Sources of Personal Data](#)
- [4. Purposes of Processing Personal Data](#)
- [5. Personal Data Disclosed and the Categories of Recipients](#)
- [6. Sale or Share of Personal Data/Use for Targeted Advertising](#)
- [7. Your Rights Under U.S. Privacy Laws](#)
- [8. How You May Exercise Your Privacy Rights](#)
- [9. Children Under Age of 16](#)
- [10. Other California Notices](#)
- [11. Information Retention](#)
- [12. Amendments to this U.S. Notice](#)
- [13. Contact Us](#)

1. Personal Data and Sensitive Data

“**Personal Data**” means information that is linked or reasonably linkable to an identified or identifiable individual. Personal Data does not include publicly available information and information that cannot be reasonably linked to you, directly or indirectly, such as de-identified or aggregated data, and information excluded from the application of U.S. Privacy Laws, such as that governed by other superseding state or federal laws As used

in this U.S. Notice, the term “Personal Data” includes “Personal Information” as defined under the CCPA.

“**Sensitive Data**” means Personal Data that a particular U.S. Privacy Law designates as “Sensitive,” which generally includes Personal Data revealing racial or ethnic origin, religious beliefs, mental or physical health history, condition or diagnosis, sex life or sexual orientation, citizenship or immigration status, genetic or biometric data that can be processed/is processed to uniquely identify an individual, precise (GPS) geolocation, and personal data from a known child. In California, Sensitive Data also includes a consumer’s social security, passport, or other government-issued ID number, a consumer’s online or financial account number along with the password or other credentials allowing access to it, and the contents of a consumer’s mail, email, or text messages, unless the business was the intended recipient. In addition, your use of AI features such as summaries, polish messages, instant answers, or other AI in-chat or chatbot features, may also involve information that could be considered sensitive and personal in nature, if you choose to provide it.

2. Categories of Personal Data or Sensitive Data We Collect

The operation and use of Viber App and Services involves collection of Personal Data, where the types of such data depend on the type of Service and interaction with us. For example, when you sign up and create an account, you directly provide us with your Personal Data. We also automatically collect certain Personal Data from your device. We explain which data we collect and how we collect it below.

The types of Personal Data collected through use of our Services, including App and website, are listed below. We note that some types of Personal Data we collect are required for all Viber Services (for example, your phone number), some types may be required solely for certain Services or features you decide to use (for example, Viber chatbots), and some are optional, and subject to your discretion (for example, your photo).

We do not read, listen to or store your messages and/ or calls made privately:

We wish to clarify that we do not read or listen to the content of your messages and/or calls made privately via Viber and we do not store those messages (including any media files transferred therein) once they have been delivered to their destination (which on average takes less than one second). If for some reason the message was not delivered to its destination within up to 2 weeks, it will be deleted from our servers. We note that we allow you the option to back up your chat history data on your own external data backup service (like iCloud or Google Drive) – see [here](#) for more info on backup, which is not collected or maintained by Viber.

Data provided or collected through registration & under your Viber account or participation in Viber's activities:

- **Identifiers**, such as:
 - Your mobile number (including mobile country/network code);
 - Your personal details (e.g., name, date of birth), if you provided them;
 - Your contact details (e.g., email address), if you provided them;
 - Your account login details, such as your username and any of your password or security pin-code, which you have chosen, if any;
 - Device identifiers, as described below.
 - **Your photo**, if you provided it (e.g., any avatar).
 - **Your phone address book**, meaning, the names, the phone numbers and the favorites list from your contact lists, if you approved access to them.
 - If you choose to use our business accounts services, any personal data included in your **business account data**.
 - Interests you choose to provide voluntarily.

Geolocation data:

- **General location**, we use IP addresses we collect and additional data (e.g., phone number area codes), to estimate your general location (e.g., city level); we may also use your residential address, if it's been provided by you.
- **GPS based location**, we will collect the GPS location for very specific purposes (as detailed below), and solely if you gave us permission, and where required, if precise location is strictly necessary to provide the service or feature.

Financial information provided or collected through your use of purchased subscription, paid features and offers:

- **Purchased subscriptions, products or services:**

If you purchase credit, paid features or subscribe to our Premium Services (e.g. a Viber Out, Viber Plus and other applicable plans) on our App or websites, we will process your billing data (e.g., full name or your user name, phone number, payment method), as well as transactions-related information (e.g., the purchasing amount, date of purchase, currency, plan information, transaction result, IP address, country, first and last 4 digits of your credit card).

- **Viber Chatbot Payment Transactions:**

- - Transactions-related details (transaction ID, time and date of purchase, purchase description, purchase amount, currency, the merchant transaction result, user free text entered information)
 - Hashed pin code

Data we collect automatically from your device, e.g., data collected using cookies and other device identifying technologies ([‘Viber Ads, Cookies and Tracking Technologies’](#)):

- **Device identifiers**, meaning identifiers of the devices you have used to access our websites and application, including IP address, unique device identifiers (including hashed phone numbers/emails), advertising related identifiers, MAC identifiers. Unique identifiers tell your device apart from other users and may be assigned to your device by Viber or our advertising service providers/partners.
- **Electronic network activity data**, such as data stored on log files, when you access our Service and website for example, including access time and date stamp, pages viewed, IP address, the pages that directed you to our website, data related to errors and crash reports.
- **Activity data**, relating to your usage of Services, such as connection status, whether you have received and seen messages sent to you, if you are currently on another call and data related to the calls and messages that you send and receive, such as length of the call, who called whom, who messaged whom, and at what time, your personal preferences related to such usage (for example how often, for how long, what options are selected, etc.). Such activity data may also include:
 - Groups, communities, channels, bots (including AI assistants), businesses, and links you interact with inside Viber – e.g. data about the groups, communities, business accounts, and channels you visit, follow or manage, messages you like, messages you send, the content you post or view, links you click on;
 - Items you searched on and shared via Viber features;
 - Offers selected or redeemed;
 - Viber Premium Services, or business accounts activity.
- Other device data, e.g., data about your device’s operating system, your browser, browser or operating system language, your wireless network, your mobile carrier, your privacy-related settings.

For more information regarding how we and our partners use cookies, as well as your choices and controls, please see our [Viber Ads, Cookies and Tracking Technologies Policy](#).

Data we collect or receive from other sources and inferred data:

- **Social media data:**
 - If you have signed in to the app through third party social media sites – your email address, birthday and gender – if such information has appeared on your social media profile – was collected. Note that we disabled the option to sign in to the app through user social media accounts, and we no longer have any access to the current data from the social media accounts of users, who have signed in to Viber in such fashion in the past.
- **Your contact name**, as saved on other users' devices if they chose to share their contacts with us.
- **Viber may also process inferences about your account and device identifier**, such as:
 - Inferred gender – for example, inferred from your name;
 - Inferred interests – inferred from your activity, such as the communities, channels, bots, businesses, other Viber services, features and links (including the public content accessible through them) you interact with inside Viber and from other Data provided or collected through registration & under your Viber account or participation in Viber's activities. For example, your general location, travel patterns inferred from it, device type, and activity data within our services may be used to infer your income level;
 - Inferences from third party data and ads-related interactions – we may receive inferred data, linked to your device identifier (mainly, a unique device identifier generated by cookies, pixels, or other tracking technologies used on our website and Services) from our third-party advertisers and service providers. Such inferred data we receive may include inferences about your interests and characteristics, generated by such third parties from other websites and services you have visited (for example whether you are interested in fintech, cars, etc., which income group you might belong to, as well as the locations you tend to visit, based on your GPS location). In addition, inferences can be generated from data on how you interact with ads displayed on our App after clicking on them and data about your activity and preferences derived from the

clicks on our own ads (and the subsequent installs of our App) associated with your device identifier, delivered on third-party advertising platforms by our ad providers. For more information, please see our [Viber Ads, Cookies & Tracking Technologies Policy](#).

- Viber does not make or process inferences using Sensitive Personal Data or about Sensitive Personal Data characteristics.

User Submitted Content:

If you choose to participate in Viber's activities (e.g., contests), or as part of your participation in communities/channels/bots' activities available on Viber, you may voluntarily publish, submit or post content such as videos, images, graphics, text, videos, etc. which may include personal data (e.g., an image of a person).

AI Features:

When you use features like summaries, polish messages, instant answers, or other AI in-chat or chatbot features, we process your text messages to provide you with the translated or summarized message, or to provide relevant responses or suggestions. This may include information that could be considered sensitive and personal in nature, if you choose to provide it. We may retain your AI assistant chatbot communications to ensure your interactions are safe and prevent harm to you or others.

Data we collect from your communications with us, including support, customer services and other inquiries:

If you choose to contact us through any means of communications we make available, you may provide us with certain data such as your contact details (e.g., name, email, phone number, mobile carrier, country – mainly where you are not a user of our Services) and other data you voluntarily wish to provide (mainly, related to the issue you wish us to address or resolve, including without limitation, information related to disputed transactions). We will further store our contact history and correspondence with you according to our retention policies.

When you submit feedback, ideas, suggestions, information or other communications to us through our Services, we may collect any personal data if you choose to provide it.

Non-User Data:

Mobile phone number and contact name, as saved on a Viber user's phone address book: We may process your mobile phone number even if you are not a Viber user, in the event that your phone number was included in our existing user's address book that has been provided to us (and subject to such user providing us with approval to access the device address book). We will also save the name it was saved under by our user. We do it to show our user who in their contacts is already using our Services and

who is not, to allow users find and communicate with their contacts who are users or who are not users in a more efficient way, and solely for as long as a relevant Viber user's account exists on Viber. In the event you will become an active user, the existing users whose phone book included your number, will be notified that you have joined the Service and you will be automatically added to their contact list within the Viber App.

If you are not a Viber user and would like to exclude your phone number, please contact us at <https://vb.me/ContactUs>

Caller ID: Your phone number and contact name (if provided to us by a user through sharing their contacts or otherwise) may be added to our Caller ID database and used as part of the caller identification under Viber Caller ID feature. Your name can be indicated to Caller ID users when you are on a call with them outside Viber or used to show them a probability of spam, if such number has been marked as spam by users. Such process enables Viber to improve our services with the purpose to reduce spam, fraud and harassment for our users.

To opt-out from the caller identification processing as described above, please visit [this page](#).

Business partners data:

When you communicate with us for business purposes as a business partner of ours, we will save your contact data provided by you (e.g. names, phone number, email address, address), as well as any correspondence we have had. We use trusted third-party providers to manage the maintenance and storage of such data.

If your business account is connected with your Viber payment services wallet, we will collect in addition:

- your ID or certificate of registration with relevant authority;
- address of your business and contact details (e.g. email and phone number);
- tax information (e.g. certificate of registration with relevant authority, TIN).

In the preceding twelve (12) months, we have collected the following categories of Personal Data, under the relevant CCPA categories:

Category	Examples	Collected
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	Yes: real name (if a user provided it), mobile phone number, unique personal identifier, online identifier, Internet Protocol address, email address (if a user provided it), account name, photo or unique avatar (if a user provided it), device identifiers.
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	Yes: name, telephone number, photo (if user provided it)

<p>C. Protected classification characteristics under California or federal law.</p>	<p>Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).</p>	<p>Yes: Age (if a user provided DOB).</p>
<p>D. Commercial information.</p>	<p>Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.</p>	<p>Yes: Viber services purchased, purchase history, plan information, transaction details, potential product or business interests (inferred).</p>
<p>E. Biometric information.</p>	<p>Genetic, physiological, behavioral, and biological characteristics.</p>	<p>No</p>
<p>F. Internet or other similar network activity.</p>	<p>Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.</p>	<p>Yes: Search history, browsing history, ads you have interacted with, clickstream data, directing URLs, call, message, and activity metadata, operating system and browser specifications, wireless network and mobile device and OS specifications.</p>
<p>G. Geolocation data.</p>	<p>Physical location, approximate location derived from IP address or movements.</p>	<p>Yes: approximate location derived from IP address or precise location derived from the user's GPS (if a user allowed it).</p>

H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	No
I. Professional or employment-related information.	Current or past job history or performance evaluations.	No
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records maintained by an educational institution.	No
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	Yes: gender and user's interests.
L. Sensitive Personal Information.	Government-issued identifying numbers, financial account details, genetic data, precise geolocation, race or ethnicity, religious or philosophical beliefs, union membership, mail, email, text messages, biometric data, health data, sexual orientation or sex life, neural data, and all personal information of consumers known to be under 16 years of age.	Yes: user's precise geolocation derived from the user's GPS (if a user allowed it).

3. Categories of Sources of Personal Data

We may collect personal data directly or indirectly from you, automatically, or from other sources.

We obtain the categories of personal data listed above from the following categories of sources:

- Directly from you, for example, when you register to our Services, you may provide us with your information such as your phone number, name, photo, etc.;
- Indirectly from your device, such as Device Identifiers (IP address, etc.), your login sessions, activity data, etc.;
- Other sources, such as social media sites if you choose to sign in through your social media account;
- Third-party service providers and partners such as analytics providers and advertising partners.

4. Purposes of Processing Personal Data

At Viber, we use your Personal Data to provide you with the best possible Service. This includes administering your account, customizing and improving the Service we offer, processing payments, serving ads and marketing campaigns, providing you with support and for compliance and safety reasons. We explain below the purposes for which we collect and use your Personal Data. We will not collect additional categories of Personal Data or use the Personal Data we collected for incompatible purposes without providing you notice.

Authentication and Account Administration:

Viber uses different types of your Personal Data such as: identifiers, your photo and phone address book, contact information, device information, etc. for the purpose of creating and administering your Viber account in order to enable you to register, log in, activate and use the Services. These include, for example:

- To authenticate and verify your account, as well as to make sure you do not already have a Viber account;
- To synchronize your contact list on the App;
- To create your profile, customize your Viber account according to the information you have provided (e.g. name or photo), and display such information as part of your profile when you use Viber Services.

Providing our Services – Communication & Content Features and enabling backups:

Viber uses different types of Personal Data in order to operate, provide and deliver to you our Services, including communication features. This includes, for example:

- To allow mobile carriers to connect calls to you and from you;
- To show your online status;
- To enable you to send and receive messages, participate in Viber calls, delete messages;
- Offer additional Viber features or enable you to only use features that are available in your location;
- Enable you to upload and create backups of your messages on external services;
- Enable you to post and share your content, images and videos, within the communities, channels, and bots;
- Subject to the permission you provide, enabling you to share your location with your contacts or enabling location-based services for you;
- Send you operational related and service-related communications, including administrative messages that relate to your use of the Services such as missed call notifications;

As stated above, your messages will not be stored by us once they have been delivered.

Enabling Paid Services: Viber Out Credit, Premium Services' Subscriptions and Paid Features, and Viber Chatbot Payments:

Viber uses different types of Personal Data in order to enable your use of the Viber Out Credit, other paid features and purchase of Premium Services' subscriptions on our App or website, including for verification purposes. This includes, for example, sharing your email address with our third-party Payment Service Providers, to enable the processing of your payments. Your credit card number will be provided by you directly to the applicable Payment Service Provider and Viber will not have unmasked access to this data. We will further store a log that will record your purchase for operational and fraud detection purposes, and such log will include your IP address or other unique identifier.

We also use certain types of data to enable you to interact with and pay third-party merchants through your use of the Viber Chatbot Payments. This data will be used solely for fulfilling our role as an intermediary and we will share with Google Pay or Apple Pay or any other linked payments provider. To enable your use of this feature, we process transactions-related details including shopping history (time and date of purchase, purchase description, purchase amount, currency, the merchant, etc.) for your record keeping and ours, as required by law. The confirmation of the payment is provided directly to the merchant and Viber does not receive or share any payment data

or registration data from Apple Pay nor Google Pay. Note that your use of Apple Pay and Google Pay, including their use of your data, is subject to their respective terms and privacy policy, which can be found here: [Google Pay](#), [Apple Pay](#).

Enabling and Managing Your Participation in Contests & Marketing Activities:

If you voluntarily choose to participate in contests and other marketing activities offered by Viber, we will use different types of Personal Data, depending on the applicable activity, in order to enable your participation and operate such activities. This includes, for example:

- If you choose to participate in a contest which involves a prize, we will request you to provide your physical address in order to ship it to you;
- The content submitted through the contest, to the extent it includes Personal Data;
- As some contests or activities are applicable solely to specific regions, we will use your general location (for example, according to your phone number area code), to validate your eligibility to participate in a specific contest.

Improving and Customizing the Service and Analytics of Viber Activity:

Viber uses different types of Personal Data, including user feedback you choose to provide or communications to us, in order to improve, enhance and evaluate the Services, as well as customize the Services, subject to your consent, where applicable, for any Sensitive Data. This may include, for example:

- We use activity data, device identifiers, IP-based location, user feedback you choose to provide or communications to us and GPS location (with your permission) to fix and evaluate the technical functionality and availability of the Services, as well as for statistical analysis of the usage and functionality, product development, continued improvement of existing features and provision of certain features;
- We use your data provided through registration and inferred data (such as inferred gender, and inferences from ads-related interactions), interests and general location to customize content we show you, including customizing our offers of certain services;
- When we advertise our Services to you on third-party platforms, we might receive indications of which advertisement led you to join our Service based on unique device identifiers associated with your device, in order, among others, to assess the performance of our campaigns, to look for similar users, for better ad measurements, as well as to learn more about your activity and preferences on our Services;

- Data collected automatically from your device or through cookies and pixels;
- Data we collect from other sources and inferred data, such as social media data, your contact name and inferences about your account and device identifiers.

Marketing Communications with Viber's Users & Location based Offers:

Viber uses different types of Personal Data in order to contact you with marketing and offers relating to products and services offered by Viber, (including your contact information and interests, if the offer is tailored to your interest) or Sensitive Data, such as GPS location, subject to your consent. This may include, for example:

- We will use your email address, name, inferred gender, age range, device and activity data, for the purpose of contacting you with marketing and offers relating to products and services offered by Viber, and our partners. When advertising Viber services outside of Viber, we might share your email address or device identifiers with our marketing vendors;
- Your IP address will be used to extract your general location (city level), for the purposes of presenting offers applicable to your region and, subject to the permissions you have provided, we may use your GPS location data for the purpose of providing you with location-based marketing offers and communications.

Please note that even after you have chosen to unsubscribe from marketing communications (see how you can do it in "[Your Choices](#)" section of [Viber Privacy Policy](#)) we may send you service-related communications, including administrative messages that relate to your use of the Services.

Advertising:

Viber uses different types of Personal Data in order to provide our advertising services (meaning, to enable the display of advertisements, including personalized advertisements provided by Viber or third-party advertisers, in our App and Services), to measure and optimize the performance of ads and deliver more relevant ads, subject to your opt-out, as applicable. This may include, for example:

- Viber will use and may share your device identifiers (mainly, a unique device identifier generated by cookies or other tracking technologies used on our website and Services, or other identifiers that tell your device apart from other users and may be assigned to your device by Viber or our advertising service providers/partners), as well as age range, inferred gender, and reduced IP address (or GPS location data, with your permission) with third party advertising partners, for the purpose of presenting you with personalized ads;

- Viber device identifiers (mainly, a unique device identifier generated by cookies or other tracking technologies used on our website and Services, or other identifiers that tell your device apart from other users and may be assigned to your device by Viber or our advertising service providers/partners), age range, inferred gender, and reduced IP address (or GPS location data, with your permission) for the purpose of presenting you with personalized ads; and
- Activity data and information we receive from third parties on your activity outside of Viber.

You can always opt out of personalized advertising by switching on the “Do not sell or share my personal information” toggle, in which case we will not share your Unique Identifier (as defined above) with our third-party advertisers. Note that you may not see this toggle in the Viber App if you have not enabled App Tracking requests in the Apple settings for iOS devices, but in such cases Viber’s tracking and sharing is already turned off. If you are having trouble finding the “Do Not Sell or Share My Personal Information” toggle you can send us an Opt-Out request at any time via the following link:

<https://support.viber.com/customer/portal/emails/new?type=CA>.

Customer Service:

Viber uses different types of Personal Data in order to provide customer service and customer support. This may include, for example your contact information, the details of your support communication, etc.

B2B Communications and Services:

We will use Business Partners Data for the purpose of communicating with you, or as otherwise needed to facilitate our engagement, as well as to send you our marketing offers. You have the ability to opt out of our direct marketing emails at any time (see how you can do it in “Your Choices” section of Viber Privacy Policy). Email addresses provided as part of the access to Viber business related features and APIs are collected and processed to enable your access to such features and APIs, enable account functionality, provide visibility and tracking of account actions (such as template management and deletions), maintain the security of account activity, and for fraud prevention and investigation purposes. Login data for Viber’s internal resources (e.g. secure portals and knowledge bases) is collected and processed to manage and secure your access to such resources. We also process Business Partners Data to analyze how our business services are used and to improve our service offering.

Safety, Security & Fraud Prevention:

Viber uses different types of Personal Data for security purposes such as fraud and spam prevention. This may include, for example: messages reported by other users, Identifiers, you name and contact information, etc.

Defending our Rights; Enforcing our Policies & Compliance with Legal Obligations and Public Interests:

Viber may use and share different types of Personal Data (or Sensitive Data if it includes your GPS location), and depending on the circumstances, for the purpose of defending our rights and enforcing our policies, terms and agreements, where it is necessary to comply with legal obligations to which we are subject and for cooperation with regulators and law enforcement bodies (where there is a valid legal request such as binding order), as well as in very limited and rare circumstances, where we find it necessary and essential for the purpose of protecting your or third party's life safety and security as well as humanitarian purposes.

5. Personal Data Disclosed and the Categories of Recipients

We disclose Personal Data and Sensitive Data as necessary with other parties, including our corporate family, service providers, advertisers (subject to opt out), and with trusted companies that help us provide our Services, in compliance with strict data security and privacy practices. We may also share Personal Data or Sensitive Data in limited circumstances where we are required to do so under applicable law. You can find below information about the categories of such recipients, as well as the purpose for which Personal Data and/or Sensitive Data is shared with such recipients.

The Viber Corporate Family:

We may share the Data we collect about you with the Viber corporate family, including our parent company, Rakuten Group Inc., and its and our affiliates (as listed [here](#)). The purposes for sharing include providing joint content, support, preventing illegal actions, corporate administration and operating the Services.

Our Service Providers and Partners:

We share your Personal Data or Sensitive Data with our trusted service providers and business partners that perform business operations for us on our behalf (as data processors) and pursuant to our instructions and a data processing agreement. This includes the following types of service providers:

- **Advertising and marketing service providers**, who help us with advertising measurements and app installations;
- **Advertising Partners**, to enable the limited advertisements on our Services, we may share device identifiers (i.e., an advertising identifier associated with your device or identifiers that tell your device apart from other users and may be assigned to your device by Viber or our advertising service providers/partners) with our third-party or affiliate advertising partners (listed [here](#)), along with certain of your device data (e.g. language preference), age range, inferred gender, country, city, reduced IP address (or GPS location data, with your permission)

and certain technical or aggregated data about you and the device you are using. This includes partners managing our advertising placements and also advertisers themselves and their agencies or third parties managing their advertising demands. Your unique advertising identifier is created by your mobile device's operating system and you can change it or choose not to share it at any time. If you want to know more, read our [Viber Ads, Cookies and Tracking Technologies](#).

- **Data storage providers**, with whom we entrust the hosting and storage of our data;
- **Customer support providers**, who help us perform such functions as customer support and customer service;
- **Data analytics and data management providers**, who help us analyze, improve, personalize, enhance our Services and moderate the content;
- **AI service providers**, which enable AI features on our app, including summary, in-chat assistance and chatbot features;
- **Measurement partners**, who help us with measurements, tracking and targeting;
- **Payment and fintech services providers**, who enable processing payments and fintech actions on our App;
- **Network and telecommunication partners**, who help us support communications and other services to users;
- **Data security partners**, who help us detect and prevent potentially illegal acts, violations of our policies, fraud and/or data security breaches and ensure compliance with legal obligations.

Where we share data with service providers and partners, we ensure they only have access to such information that is strictly necessary in order for us to provide the Services. When we disclose Personal Data for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that Personal Data confidential and not use it for any purpose except performing the contract. We further restrict the contractor and service provider from selling or sharing your Personal Data.

Third-Parties Offering Service Through our App:

As part of Viber's Services, we allow third parties to create communities and channels on Viber, and develop, through the use of Viber's API, their own bots, chat extensions and integrate into Viber explore screen in order to communicate with Viber users ("**Third Party Communications**"). In the event you voluntarily choose to interact with the Third-Party Communications through your use of the Services, such third parties may receive

certain data about the user, such as your user's name, photo, country, some device data and Viber unique ID. These third parties are **not** processing the data on our behalf, meaning, their use of your data shall be subject to their policies and privacy practices.

Legal and Law Enforcement:

Subject to our strict data security and privacy practices and without compromising our end-to-end encryption, we may disclose certain types of your data, including, and depending on the circumstances, activity data, Identifiers and your phone address book, to law enforcement, governmental agencies, or authorized third parties, in response to a verified request relating to terror acts, criminal investigations or alleged illegal activity or any other activity that may expose us, you, or any other Viber user to legal liability, and solely to the extent needed to comply with such purpose.

Corporate Transactions:

In the event of a corporate transaction (e.g., sale of a substantial part of our business, merger, consolidation or asset sale) we will share the data we store with our acquiring company. We will obligate the acquiring company to assume the rights and obligations as described in this Privacy Policy (including this notice), and we will notify you of such corporate changes in your data processing.

To see what other Viber users can see about you when you use our services, check [What Other Users Can See](#) section of Viber [Privacy Policy](#).

6. Sale or Share of Personal Data/Use for Targeted Advertising

We do not collect your Personal Data for the purpose of selling it in exchange for money; however, we do enable placement of third-party advertisements through our Services and share certain Personal Data for such purpose, which may amount to a "sale" or "share" of your Personal Data (or Personal Information) under the CCPA's broad definition of the term (the CCPA defines "sharing" as "communicating orally, in writing, or by electronic or other means, a consumer's personal information" to "a third party for cross-context behavioral advertising, whether or not for money or other valuable consideration."), or would constitute the processing of your Personal Data for Targeted Advertising under other applicable U.S. Privacy Laws, which is subject to your right to opt-out where applicable. In other words, we may share your Personal Data (or Personal Information) with a third party to help serve ads that may be more relevant to your interests, and to perform other advertising-related services such as enabling our partners to serve such personalized content, unless you opt out.

To enable the limited advertisements on our Services, we may share Device Identifiers (e.g., an advertising identifier associated with your device, or a unique identifier that tells your device apart from other users and may be assigned to your device by Viber or our advertising service providers/partners) with our third-party advertising partners

(listed here), along with certain of your device data (e.g., language preference), age range, inferred gender, country, city, reduced IP address (or GPS location data, with your permission) and certain technical or aggregated data about you and the device you are using.

In the preceding twelve (12) months, we “sell” or “share” or process for the purposes of “Targeted Advertising” the following categories of Personal Data:

Category (corresponding with the table above)	Category Recipient	Purpose of Sale or Share
Category A (Identifiers)	Ad-network	Share for cross-context behavioral advertising
Category F (Internet or other similar network activity)		
Category G (coarse geolocation data)		
Category K (Inferences drawn from other personal information)		
Category L (Sensitive Personal Information, specifically precise geolocation)		Share for cross-context behavioral advertising (if user consents).

7. Your Rights Under U.S. Privacy Laws

Subject to U.S. Privacy Laws and your interaction with Viber, you may have certain rights regarding the Personal Data that Viber Collects about you. Such rights may include the right to know or confirm which types of Personal Data we collect and why we collect it (as we detail under this U.S. Notice), the right to access your Personal Data that we hold about you, the right to request correction of inaccuracies in your Personal Data, the right to request us to delete your Personal Data, the right to opt-out of certain data collection, sale, or uses, as well as the right to appeal Viber’s decision regarding your rights. We further explain below the operational meaning of each such right as provided under applicable U.S. Privacy Laws, as well as when and how you may exercise your right.

Right to Access/	You have the right to confirm and know the Personal Data	You can exercise your right by reviewing this Privacy Policy, you may access and
-------------------------	--	--

<p>Right to Know</p>	<p>we collected from or about you and the right to Access a copy of the Personal Data.</p>	<p>request a copy of the specific Personal Data collected by us about you by tapping the “request your data” button in Viber’s privacy settings on your App. Once the copy is ready, you will receive a file from Viber containing this information. If you have further questions, please contact us.</p>
<p>Right to Correction</p>	<p>You have the right to correct inaccuracies in your Personal Data, taking into account the nature of the Personal Data and the purposes of the processing of your Personal Data.</p>	<p>You can exercise this right directly through the Viber App, we enable you to delete, edit/correct your messages anytime, even after they have been sent (they will be deleted or appear edited for you, your friend and our Services).</p> <p>You can delete and correct any information available in your account, through the App settings as detailed here: https://help.viber.com/hc/en-us/articles/9062953104029-Request-Review-and-Delete-Your-Data-on-Viber</p>
<p>Right to Deletion</p>	<p>You have the right to delete your Personal Data, although this right is not absolute and in certain circumstances we may deny such request where provided by the relevant U.S. Privacy Law.</p>	<p>You do not need to create an account with us to submit a request to delete.</p> <p>You can exercise your right to erasure in the following ways:</p> <p>Delete your account or service-specific profile. Deleting your Viber account is the most comprehensive way to erase your Personal Data from our servers. You can deactivate your account through your Viber settings, and upon deactivation, your data and chats will be automatically deleted from your devices. We will delete all data associated with your account, except data we are required to retain under applicable law (such as financial records and certain</p>

		<p>activity logs, as described in our Data Retention section of Viber’s Privacy Policy). If you use specific Viber services that maintain a separate profile (such as a Business Account), you may delete your data either through removing the information from the non-mandatory fields of your service-specific profile or delete that service-specific profile entirely without deactivating your main Viber account.</p> <p>Delete your data while continuing to use the App. We have made it easy for you to request deletion of your historical Personal Data from our servers while keeping your Viber account active. Simply tap on the ‘Personal Data > Delete Your Data’ button in your privacy settings. We will delete the data which we are not otherwise required to keep or is not necessary for the provision of the Service. For a full description of what is and is not deleted through each method, check our support articles. When you request deletion to Viber, we will delete or de-identify Personal Data not subject to one of the listed exceptions from our records and will direct our processors to take similar action.</p>
<p>Right to Portability</p>	<p>You have the right to obtain the personal data in a portable, and to the extent technically feasible, readily usable format that allows you to transmit the data to another entity without hindrance.</p>	<p>You may request to receive a copy of your Personal Data, including specific pieces of Personal Data, including, where applicable, to obtain a copy of the Personal Data you provided to us in a portable format.</p> <p>We will select a format to provide your Personal Data that is readily usable and should allow you to transmit the</p>

		information from one entity to another entity without hindrance.
<p>Right to opt out from (i) selling Personal Data; (ii) Right to opt out from processing for Targeted Advertising ; and (iii) Right to opt out from profiling</p>	<p>You have the right to opt out of the processing of your Personal Data for the purposes of targeted advertising, its sale to a third party for monetary gain or other value, or for profiling in furtherance of decisions that produce legal or similarly significant effects concerning you or any other consumer.</p> <p>You may authorize another person acting on your behalf to opt out (including by technical tools and opt out signals).</p> <p>To enable the limited advertisements on our Services, we may share Device Identifiers (i.e., an advertising identifier associated with your device) with our third-party advertising partners (listed here), along with certain of your device data (e.g., language preference), age range, inferred gender, country, city, reduced IP address (or GPS location data, with your permission) and certain technical or aggregated data about you and the device you are using.</p>	<p>You can choose to allow or to not allow customization and personalization of our Services provided to you based on your Personal Data, by changing your personal data toggles in the privacy setting within the App.</p> <p>You can simply open the Viber App, access the “Settings/privacy/personal data” menu within the App and switch the “Do Not Sell or Share My Personal Information” toggle on (the “Opt-Out”).</p> <p>Note that you may not see this toggle in the Viber App if you have not enabled App Tracking requests in the Apple settings for iOS devices, but in such cases Viber’s tracking and sharing is already turned off. If you are having trouble finding the toggles or need further instructions you can send us an email to privacy@viber.com, or contact us via our online form as described below. Furthermore, if you are having trouble finding the “Do Not Sell or Share My Personal Information” toggle you can send us an Opt-Out request at any time via the following link: https://support.viber.com/customer/portal/emails/new?type=CA</p> <p>You can also make additional choices on your phone’s settings by changing our App’s permissions such as to allow or disable GPS location sharing, access to contact list and more.</p> <p>We recognize valid opt-out preference signals sent from browsers, including the Global Privacy Control, on our websites.</p>

		<p>When we receive such signals that do not conflict with your existing privacy preferences, we will automatically exercise opt-out rights that may be available to you under applicable U.S. State privacy laws, such as the rights to opt out of sale, sharing, and processing your personal information for targeted advertising, for your browser. One way that you can use such opt-out signals is by following the instructions for your device or browser located here: https://globalprivacycontrol.org.</p>
<p>Right to Limit the Use or Disclosure of Sensitive Personal Information</p>	<p>For California residents, under certain circumstances, if the business collects or discloses Sensitive Personal Information and uses Sensitive Personal Information with the purpose of inferring characteristics about a consumer, you have the right to limit the use or disclosure of Sensitive Personal Information by the business.</p>	<p>As stated, Viber does not make inferences using Sensitive Personal Data or about Sensitive Personal Data characteristics. However, Viber offers you the ability to control our collection and disclosure of your precise geolocation. You may opt-out from GPS precise location processing through your mobile device settings. Further, note that if you disable App Tracking in the Apple settings for iOS devices, Viber’s tracking based on GPS precise location for cross-contextual behavioral advertising will be turned off.</p>
<p>Right to Appeal</p>	<p>If we decline to take action on your request, we shall so inform you without undue delay, within 45 days of receipt of your request, unless a sooner time is required by a particular U.S. Privacy Law. The notification will include a justification for declining to take action, which determination you may appeal to Viber.</p>	<p>In the event that we decline to take action on or deny your request to exercise your rights, you may have the right to appeal our decision, depending on your state’s law. Please send your appeal request with a summary of the request and decision you want to appeal to privacy@viber.com.</p> <p>Within 45-60 days after receipt of an appeal, depending on your jurisdiction, we will inform you in writing of any action taken or not taken in response to the</p>

		appeal, including a written explanation of the reason for the decisions and, if the appeal is denied, a method by which you can complain to the relevant state authority.
Duty not to retaliate or violate the existing laws against discrimination or non-discrimination	We must not process your Personal Data in violation of existing laws that prohibit unlawful discrimination against consumers nor discriminate or retaliate against you for exercising your privacy rights, such as denying a good or service, providing a different level or quality of service, or charging different prices, except where such different treatment is justified by the lack of personal data required to provide such services.	We do not process data to discriminate nor discriminate or retaliate against our users for exercising their privacy rights.

8. How You May Exercise Your Privacy Rights

Rights that can be exercised directly through the Viber App settings or Viber accounts:

- We enable you to delete, edit/correct your messages anytime, even after they have been sent (they will be deleted or appear edited for you, your friend and our Services).
- You can also control your privacy settings within the App to change the visibility of your online status.
- You can disable the “seen” notification so that other users do not know whether you’ve read a message yet.
- You can choose not to share your photo and/or birthday or not to allow other users to look you up by name, which choices are available within the App.

- You can also make additional choices on your phone's settings by changing our App's permissions such as to allow or disable GPS location sharing, access to contact list and more.
- If you do not wish to receive Viber marketing notifications, you may adjust your system settings to decline notifications from Viber, or submit a request to our support. And if you subscribed to receive promotional emails from Viber, you can unsubscribe in any such email at any time.
- Sending a message to a bot or subscribing to a bot will allow admins of that bot to send you notifications and personal messages. If you do not wish to receive such notifications, you may adjust your account settings to decline them or opt-out at any time from receiving further notifications. You may also adjust your phone preferences to enable or disable the use of your GPS location data at any time.
- You can choose to allow or to not allow customization and personalization of our Services provided to you based on your Personal Data, by changing your personal data toggles in the privacy setting within the App.

Opt Out from cross-contextual ads or use of GPS precise location in cross-contextual ads:

You can simply open the Viber App, access the "Settings/privacy/personal data" menu within the App and switch the "Do Not Sell or Share My Personal Information" toggle on (the "Opt-Out"). Note that you will not see this toggle in the Viber App if you have not enabled App Tracking requests in the Apple settings for iOS devices, but in such case Viber's tracking and sharing, including processing of GPS precise location in cross-contextual ads is already turned off. Note in any event you can opt-out from GPS location processing through your mobile device settings. If you are having trouble finding the toggles or need further instructions you can send us an email to privacy@viber.com (opens in a new tab), or contact us via our online form as described below. Furthermore, if you are having trouble finding the "Do Not Sell or Share My Personal Information" toggle you can send us an Opt-Out request at any time via the following link: <https://support.viber.com/customer/portal/emails/new?type=CA> (opens in a new tab)

Global Privacy Control

We recognize valid opt-out preference signals sent from browsers, including the Global Privacy Control, on our websites. When we receive such signals that do not conflict with your existing privacy preferences, we will automatically exercise opt-out rights that may be available to you under applicable U.S. Privacy Laws, such as the rights to opt out of sale, sharing, and processing your personal information for targeted advertising, for your

browser or account. We also indicate on our website whether a Global Privacy Control signal has been honored to effectuate your opt-out. One way that you can use such opt-out signals is by following the instructions for your device or browser located here: <https://globalprivacycontrol.org> (opens in a new tab).

In addition to the various methods described above that allow you to easily exercise your rights via your App's settings at any time, you may also submit a request to exercise your rights by contacting us, as follows:

- Our online form available at: <https://vb.me/ContactUs> (opens in a new tab) – please choose the “privacy inquiry” category.
- Using the “contact us” form on the App.
- Email: privacy@viber.com (opens in a new tab)

We may require additional information from you in order to honor your request and we may decline your request as permitted under applicable law.

We will respond to a verifiable request within the timeframes set forth under the U.S. Privacy Laws, including any extensions (in such event, we will inform you of the reason and extension period in writing). We may reply by a notification under your account, email, or other means of communication. We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded.

Authorized Agents

Please note that only you or a person that you authorize in writing to act on your behalf may make a verifiable request related to your personal information. You may also make a verifiable request on behalf of your minor child. Such request must include sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative as well as sufficient details regarding your request that allows us to properly understand, evaluate, and respond to it. Even if you submit your request via an authorized agent, we may contact you to verify your identity or validate your request, as needed.

9. Children Under Age 16

Viber does not knowingly sell, share, or process the Personal Data of the U.S. users who are under 16 years of age for cross-context behavioral advertising or Targeted Advertising. Additionally, certain features such as business accounts are strictly limited to users over the age of 18, and we reserve the right to request additional data from you to validate your eligibility to use such services.

10. Other California Notices

Notice of Financial Incentives:

We do not offer financial incentives to consumers for providing their Personal Data/Personal Information.

“Shine the Light” Requests:

California Civil Code Section 1798.83 (“Shine the Light”) permits you, if you are a California resident, to request certain information regarding our disclosure of Personal Information to third parties for their direct marketing purposes. Please email us at privacy@viber.com for more information, however please note Viber does not disclose your Personal Information to third parties for their direct marketing use within the meaning of “Shine the Light” provisions.

Do Not Track Settings

Cal. Bus. And Prof. Code Section 22575 also requires us to notify you how we deal with the “Do Not Track” settings in your browser. As of the effective date listed above, there is no commonly accepted response for Do Not Track signals initiated by browsers. Therefore, we do not respond to the Do Not Track settings. Note that Do Not Track settings are not the same as Universal or Global Privacy Controls, or opt-out preference signals, which we recognize and honor for opt-outs, as described above.

11. Information Retention

We only retain Personal Data for as long as required to fulfill the purpose(s) for which the information was collected, unless a legal obligation requires us to retain it longer. Please see the “Data Retention” section of Viber’s Privacy Policy for more details about how long we keep your Personal Data for the purposes described above.

The retention periods are determined according to the following criteria:

- For as long as it remains necessary in order to achieve the purpose for which the Personal Data was initially processed. For example: if you contacted us, we will retain your contact information at least until we will address your inquiry. We may keep measurement data and activity data on a non-identifiable basis to improve our Services and for business analytics purposes.
- To comply with our regulatory obligations. For example: transactional data will be retained for up to seven years (or even more under certain circumstances) for compliance with our bookkeeping obligations purposes.
- To resolve a claim, we might have or a dispute with you, including any legal proceeding between us, until such dispute will be resolved, and following, if we find it necessary, in accordance with applicable statutory limitation periods.

12. Amendments to this U.S. Notice

We reserve the right to amend this U.S. Notice from time to time, at our sole discretion. The most recent version of the U.S. Notice will always be posted on the website. The updated date of the U.S. Notice will be reflected in the U.S. Notice heading. We will provide notice to you if these changes are material, and, where required by applicable law, we will obtain your consent. Any amendments to the U.S. Notice will become effective immediately, unless we notify otherwise. We recommend you review this U.S. Notice periodically to ensure that you understand our most updated privacy practices.

Current United States Regional Privacy Notice March 2026

Previous [United States Regional Privacy Notice August 2025](#)

Previous [Privacy Notice for California Residents March 2025](#)

13. Contact Us

- **Our online form available at:** <https://vb.me/ContactUs> – please choose the “privacy inquiry” category.
- **Using the “contact us” form on the App.**
- **Email:** privacy@viber.com