Privacy Notice for Users in the EEA and UK under the General Data Protection Regulation

Last Updated: March 23, 2026

*View our Teens Privacy Guide **here**.*

This privacy notice provides more details to the information contained in **Viber's Privacy Policy** and applies to users in the **European Economic Area (EEA)** and the UK ("**EU Region Privacy Notice**"), in accordance with applicable laws.

This EU Region Privacy Notice provides you with information regarding our processing operations, our lawful basis to process your personal data, categories of third parties we share your personal data with, data transfer outside the European region, data retention, and as required under the General Data Protection Regulation and the UK Data Protection Act 2018 (and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) (collectively **"GDPR"**), as well as information regarding your rights related to your personal data that Viber processes when you use our Services (as detailed under **Viber's Terms of Service**), including Viber payment services (if you use it).

TABLE OF CONTENTS

- Data Controller & Data Protection Officer
- The Data We Collect
- How We Use Your Data & Lawful Basis for Processing Your Personal Data
- Data Sharing - Categories of Recipients We Share Personal Data With
- Data Transfer
- Data Retention
- Your Rights Related to Your Personal Data
- Children's Privacy
- Changes to this EU Region Privacy Notice

Data Controller & Data Protection Officer

Viber Media S.à.r.l., a société à responsabilité limitée incorporated under the laws of the Grand Duchy of Luxembourg, is the controller of your personal data.

You may contact us and our Data Protection Officer, as follows:

- **Our online form available at: https://vb.me/ContactUs** - please choose the "privacy inquiry" or "GDPR inquiry" categories.
- **Using the "contact us" form on the App**.
- **By Email**: **DPO@viber.com**
- **By mail:**
  Viber Media S.à r.l.,
  Attention: Data Privacy Officer
  2, rue du Fossé, L-1536
  Luxembourg, Grand Duchy of Luxembourg.

Back to top

The Data We Collect

The operation and use of our 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 for Viber, you directly provide us personal data. We also automatically collect certain personal data from our users' device. We explain which information 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 payment services), and some are optional, and subject to your discretion (for example, your photo).

We do not read, listen 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.

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.

Dating Data provided or collected through registration & usage of our dating services:

- **Dating Profile data –** your identification and account data, such as your name, date of birth, your gender, your dating preference gender, type of relationship you are looking for, your photos, your hobbies and interests, and any other information and content you choose to post on your dating profile such as your bio and a brief description of yourself, what are you looking to find, your habits, what you do for a living, your education.
- **Precise Location Data** – your accurate location (through and subject to your device permissions), is required and will be utilized to allow service functionality by finding you matches with the nearby participants of the dating services.
- **Dating Services Activity and Usage Data –** such as likes and dislikes of other participants' profiles, matches, profiles you hide/block, use of Premium Items and any paid features, inferences from such activities.
- **Biometric Data –** to verify that your dating profile is genuine and prevent impersonation, we process biometric data, subject to your consent, by comparing your profile photo with a selfie you provide. This involves analyzing unique facial features to determine whether the same person appears in both images, for which we only keep a score with the result of this analysis while your dating profile is active.

Special Categories of Personal Data

- As part of your registration to and usage of the dating services, we may collect and process certain types of information that could be considered sensitive and

"Special Categories of Personal Data" under the GDPR. This may include your dating preferences, and types of relationship you are looking for, which are inherently necessary for matching you with potential partners, and other sensitive information, such as your religious beliefs, which you may choose to provide at your discretion.

- Your use of Viber's AI features, like summaries, polish messages, instant answers or other AI in-chat or chatbot features, may include information that could be considered sensitive and very private in nature, if you choose to provide it.

Geolocation data:

- **General location**, we use IP addresses we collect and additional information (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 use the GPS location for very specific purposes (as detailed below), and solely if you gave us permission.

Financial information provided or collected through your use of our financial services (e.g., payment solutions), or purchased subscriptions 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, Viber eSIM 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; 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)
- **Viber payment services**:
  - Know Your Client ("**KYC**") or Know your Business ("**KYB**") data – including full name, date of birth, phone number, nationality, email, country of residence, national identity document, selfie, address and proof of address, source of funds and confirmation of the KYC verification status (i.e., approved or declined), KYC level, KYC errors, tax ID (where required in a certain country), other registration information, business name, other related documents specifically requested as part of KYC/B;

- Transaction and wallet related information – including your digital wallet balance), details of the tokenized version of the credit/debit card of the user, details of your wallet such as your IBAN, wallet ID and Swift code or wallet account, payment transaction information (including the instruction ID, payment method, fees, exchange rate, amount, currency, date, time, status of the payment, payment references, group ID, if payment in the group is made, fraud related information.).In addition, if you send or receive payments or interact with other persons, we may have access or otherwise store the sender's or recipient's account details (e.g. wallet details and bank account details (including full name, country location and IBAN and Swift/ BIC code), wallet details (including wallet ID), details of the tokenized version of the credit/ debit card, payment IDs, payment information (i.e. merchant category code, type, authorization code), payment method information, country, address, date of birth, name, phone number, email, status in a promotion);
- Utility bills payments information, such as your invoice or receipt for the utility bills, date of issue, total value, name of your utility provider, his tax number, address and payer's name.
- Hashed pin code.

Data we collect automatically from your device, e.g., data collected using cookies and other device identifying technologies ('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 information 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, information 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 who, who messaged who, 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:

- We may collect activity data about groups, communities, channels, bots (including AI assistants), businesses, dating services and links you interact with inside Viber – e.g. data about the groups, communities, business accounts, channels, and dating profiles 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 and rewards selected or redeemed; and
- Viber Premium Services, payment services activity 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, dating profiles or 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 or other tracking technologies used on our website and Services) from our trusted 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 pertain 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's advertising platforms by our trusted third parties. For more information, please see our **Viber Ads, Cookies & Tracking Technologies Policy.**

- **eSIM data**: For eSIM services, we receive data from our third-party network providers such as eSIM identifier data (e.g. ICCID, IMSI, activation code), data consumption information (e.g. data volume used and session timestamps), and location (e.g. country, network routing, MCC, MNC).

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).

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.

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 information 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 information 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.

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 Users' 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 Viber user through sharing their contacts or otherwise) may be added to our Caller ID database and used as part of (for more info see **here**). It will then be processed to display a spam indicator on calls to Viber users outside Viber, if such number has been marked as spam by users. Such process enables Viber to improve Caller ID services with the purpose to reduce spam, fraud and harassment for our users.

To opt-out from the processing 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)

Back to top

How We Use Your Data & Lawful Basis for Processing Your Personal Data

Under the GDPR, we must have a lawful basis to process your personal data. This may include collection of personal data for the purpose of performing our contract with you (for example, create your Viber account), fulfilling our legitimate interests (for example, collection of data in order to secure our Services), complying with our legal obligations, as well as, where applicable, processing personal data based on your consent (for example, when you voluntarily request to participate in our marketing activities). You can find here information regarding the purposes for which we process the types of personal data listed above, as well as our lawful basis for such processing operations.

In a summary, our lawful basis to process your personal data will be one of the following:

- **Performance of Contract**: We rely on the contractual obligations for the purpose of providing you with the Services in accordance with our **Terms of Service**, such as, enabling you to register to, log in and/or activate the Services, use and participate specific services and features such as the dating services, to back up your data in connection with in-app purchases, or limited financial services if you use these.
- **Legitimate Interest**: We rely on legitimate interest for contextual marketing campaigns or promotions based on first party behavior data (meaning, the way you interact with Viber Services), product development, continued improvement of existing features and provision of certain features, processing a non-user data for the contact list purposes, fraud/spam prevention, and in order to create your Rakuten account. When we process personal data to meet our legitimate interests, we put in place robust safeguards to ensure that your privacy is protected to ensure that the risk to your interests or fundamental rights and freedoms is minimized.
- **Legal Obligation, Compliance and Public Interest**: In some cases, we may also have a legal obligation to process your personal data such as fulfilling your user's rights or may otherwise need your personal data to protect your vital interests or those of another person.
- **Consent**: Where required under applicable law, we will obtain your consent to collect, use or share your data, including through cookies on our website or SDK and other tracking technologies embedded in the App (all as detailed in the

Viber Ads, Cookies & Tracking Technologies Policy). You can withdraw your consent at any time.

The table below details the lawful basis we rely on for each personal data set, aligned with the purpose of use. Certain types of personal data might be used for multiple purposes, and accordingly will be processed under different lawful basis.

Please note that, the actual **processing operation** per each purpose of use and lawful basis detailed in the table above, may differ. Such processing operation usually includes set of operations, made by automated means, such as collection, storage, use, disclosure by transmission, erasure or destruction, and may involve transfers of personal data to third party countries as further detailed in the Data Transfer section below.

Type of Data For full explanation, see "**The Data We Collect**" section above	**Purpose of Use**	**Lawful Basis for Processing Personal Data**
Data provided or collected through registration & under your Viber account: ● **Identifiers**, such as: • Your mobile number; • Your personal details; • Your contact details; • Your account login details; ● **Your photo** ● **Your phone address book** Geolocation: ● **General location**	**Authentication & Account Administration**	**Performance of Contract**: Our processing of this data is necessary for performing our contract with you – meaning, to create and administrate your Viber account in order to enable you to use our Services, including: ● In order to enable you to register to, log in and/or activate the Services, access Customer Support; ● To authenticate and verify your account, as well as to make sure you do not already have a Viber account, we will use your phone number to send verification notice. ● To create your profile, customize your Viber account according to the information you have provided (i.e., name, photo, etc.), and display such

Data we collect automatically from your device: ● **Device identifiers** ● **Other device data** Data collected from other sources and inferred data: ● **Social media data**		information as part of your profile when you use Viber Services.
Data provided or collected through registration & under your Viber account: ● **Identifiers,** such as: • Your mobile number; • Your personal details; • Your contact details; • Your account login details; ● **Your business account data** ● **Your photo** ● **Your phone address book** Geolocation: ● **General location** ● **GPS based location**	**Providing our Services - Communication & Content Features (messaging, voice and video calls, group chats, communities, channels, business accounts, bots, chat extensions, explore screen, stickers, Viber lenses, etc.), and enabling backups**	**Performance of Contract**: Our processing of this data is necessary for performing our contract with you – meaning, to operate, provide and deliver our Services to you and the communication features, including: ● 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. ● To provide you with other App's features such as operational notifications (e.g., missed calls). ● We will use your IP address to extract your approximate location, in order to enable you to use certain features that are only available in certain countries (for example, sticker packs). ● With your permission, to enable you to share your location in a chat or

Data we collect automatically from your device: ● **Device identifiers** ● **Electronic network activity data** ● **Activity data** ● **Other device data** Data we collect from other sources and inferred data: ● **Social media data** User Submitted Content		enabling location-based services for you. ● Enable you to upload and create backups of your messages on external services. ● Enable you to post and share your User Submitted Content (e.g., images, videos, texts) on our communities, channels, bots, dating and business services, where allowed by its administrator, and generally utilize our content features. As stated above, your messages will not be stored by us once they have been delivered. ● When you use features like messages translation, the AI in-chat or chatbot features, we process the text messages to provide you with the translated or summarized message, or to provide relevant responses. This may include information that could be considered sensitive and personal in nature, if you choose to provide it.
Dating Profile data (including Special Categories of Personal Data): • Name* • Date of birth* • Your photo(s)* • Your gender*	**Viber Dating Services**	**Performance of Contract**: Our processing of your Dating Profile Data is necessary for performing our contract with you — that is, to operate, provide, and deliver our Dating Services to you. • Enable you to register and log in to Your Dating Profile as well as to use Customer Support; • Verify your eligibility to use the Dating Services according to

• Your dating preference gender* • The type of relationship you are looking for* • Your bio • Your interests, habits and preferences if you choose to provide them ● **Biometric data, if you choose to verify your profile** ● **Precise Location Data*** ● **Dating Services Activity and Usage Data** ● **Copy of ID or similar verification documents**		our Dating Terms. As part of such process you might be required to provide a copy of your ID or similar documentation. We will not retain such copies for a period longer than required for the verification process; • Display your profile when you use Dating Services, i.e. making your dating profile available to other dating service participants; • Allow you to interact with matches on the Dating Services. **Consent**: Subject to your consent, we use your Special Categories of Data, and Precise Location Data to: • Match you with potential matches, as generated by our automatic matching system. Please note that you can always choose how much detail you provide in your Dating Profile (except for data marked with asterisk * on the left which is mandatory for the minimal experience). To withdraw your consent to us for processing Special Categories of Data, please remove or edit your profile data in your Dating Profile settings for optional data, such as religious information, and if such are part of mandatory information, please contact our **support team**.

		Subject to your permission, via your phone settings, to access your Precise Location, we will use it to suggest you potential matches in your location. Your Precise Location Data is essential for the provision of Dating Services and showing relevant dating profile to you. • Verify your Dating profile. Subject to your consent, we will process biometric data to verify your dating profile. This involves comparing a selfie you provide with your profile photo using facial recognition technology, to confirm that the person in the profile is you. This helps prevent impersonation and fake profiles by detecting your genuine presence on the other end of the device. We process the selfie and facial data to generate a verification score, a numeric result indicating how closely the images match. After verification, we only keep this verification result for possible future review (e.g. if your profile photo is edited or removed). We do not store or reuse the biometric templates or facial geometry data. This information is stored only as long as your dating profile is active. If you delete your dating profile, your verification result will also be deleted. If you change or remove the profile photo that was used during verification, your verified status will no longer apply, and you'll be asked to complete the verification process again to keep your profile marked as verified.

Data provided or collected through registration & under your Viber account: ● **Identifiers**: • Your mobile number; ● **Your phone address book** Data we collect from other sources and inferred data: ● **Your contact name**, as saved on other users' devices if they chose to share their contacts with us.	**Synchronize Your Address Book**	**Consent:** Some features, such as calls and chats, will ask you to synchronize your contact list on the App so that Viber can identify contacts that are Viber users to allow you contacting them on Viber. We will obtain your consent in order to use this data for the purpose of synchronizing your contact list (meaning, in order to show you your contacts on the Viber interface so you contact them through Viber or hide them on your dating profile if you choose so). You have the right to withdraw consent at any time, by changing the App's settings and permissions on your phone, without affecting the lawfulness of processing based on consent before its withdrawal.
Data provided or collected through registration & under your Viber account: ● **Identifiers**, such as: • Your mobile number; • Your personal details; • Your contact details. Financial information provided or collected	**Viber Out Credit, Premium Services' Subscriptions and Paid Features, Viber eSIM.**	**Performance of Contract**: We process this data when it is necessary for performing our contract with you, meaning – 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. For example, a log with your purchase will be recorded, and such log will include your IP address or other device identifier. When you purchase Viber Out Credit, paid features or Premium Services' subscriptions on our website, Viber

through your use of our limited financial services (e.g., payment solutions), or purchased subscription and offer: ● **Purchased subscriptions, products or services:** billing data (e.g., billing address, full name or user name, phone number, account, payment method), 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). Data we collect automatically from your device: ● **Device identifiers** Data we collect or receive from other sources and inferred data: • eSIM Data		may share certain information with our third-party payment service providers, such as your email address. 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. When you purchase an eSIM, we partner with trusted network and telecommunication partners, who process network connection data independently. Viber does not access the content of your communications.
Data provided or collected through registration & under your Viber account: ● **Identifiers**, such as:	**Viber payment services**	**Performance of Contract**: We process this data when it is necessary for performing our contract with you, meaning – to enable your use of the Viber payment services, and for example:

• Your mobile number; • Your personal details; • Your contact details; • Your account login details; • Country of residence; • Hashed pin code. Financial information provided or collected through your use of our limited financial services (e.g., payment solutions), or purchased subscription and offer: • Know Your Client/Business ("**KYC/B**") data; • Transaction and wallet related information; • Hashed pin code. • Utility bills payment data. Geolocation: • **General location** Data we collect automatically from your device: ● **Device identifiers**		● We must identify you in order to enable you the use of the Viber payment services; ● We will share certain KYC/B and payment data you provide with our payment service providers, and they may in turn share with downstream banks, Payment Service Providers, messaging systems, such as SWIFT to enable the payment processing. We will not share information more than is strictly necessary (some information is collected directly by the Payment Service Provider and is subject to their Privacy Policy); ● We access your IP address to verify your location and determine eligibility for services; ● App and customer support authentication; ● If you make a payment we share with the recipients some of your personal details such as your name and IBAN; ● Enabling you to pay your utility bills using Viber payment services and our Payment Service Providers; ● Enabling you to easily make future transfers to a beneficiary's bank account or wallet account, to which you have previously made a payment transfer. **Legitimate Interests:** ● We rely on legitimate interest in connection with the processing of bank account details of recipients to whom you have made a payment transfer, in

● **Activity data:** • Offers selected or redeemed.		order to enable you to easily make future transfers to such recipient's account. ● If you are a Viber user who is not registered with Viber payment services, but you interact with Viber payment services users by sending or receiving funds, or being part of a promotion, then the following information about you may be stored and used: the sender's or recipient's account details (e.g., bank account details (including IBAN and Swift/ BIC code), wallet details (including wallet ID), details of the tokenized version of the credit/ debit card, payment IDs, payment information (i.e. merchant category code, type, authorization code), payment method information, country, address, date of birth, name, phone number, email, status in a promotion.
Financial information provided or collected through your use of our limited financial services (e.g., payment solutions), or purchased subscription and offer: ● **Viber Chatbot Payment Transactions**, meaning transactions-related details including shopping history (transaction ID, time and date of purchase, purchase description, purchase amount,	**Viber Chatbot Payments**	**Performance of Contract**: We process this data when it is necessary for performing our contract with you, meaning – to enable your use of the Viber Chatbot Payments to interact and pay to third party merchants. We will use your data solely for fulfilling our role as an intermediary and we will share with Google Pay or Apple Pay or any other linked payments provider. 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,

currency, the merchant transaction result, user free text entered information).		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**.
Data provided or collected through registration & under your Viber account: ● **Identifiers**, such as: • Your mobile number; • Your personal details; • Your contact details. Data we collect automatically from your device: ● **Device identifiers** Geolocation ● **Activity data:** • Offers selected or redeemed. ● **General location** User Submitted Content	**Participation in Contests & Marketing Activities**	**Consent:** We will obtain your consent in order to use this data for the purpose of enabling you to participate in our contests or other marketing activities offered by us from time to time. You have the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Please note that the specific types of the data listed herein that we will process may vary, depending on the contest or activity type. For example, some contests may involve a prize we need to ship to you and for this we will request you to provide your physical address. In addition, some contests or activities are applicable solely to specific regions, and for this 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.
Data provided or collected through registration & under your Viber account:	**Improving and Customizing the Service &**	**Legitimate Interest:** We rely on legitimate interest in connection with our processing of this

● **Identifiers**, such as: • Your mobile number; • Your personal details; • Your contact details. Geolocation data: ● **General location** ● **GPS based location** Data we collect automatically from your device, e.g., data collected using cookies and other device identifying technologies (**'Cookies and Tracking Technologies'**): ● **Device identifiers** ● **Electronic network activity data** ● **Activity data** ● **Other device data** Data we collect from other sources and inferred data: ● **Social media data** ● **Your contact name** ● **Inferences about your account and device identifier**: • Inferred gender;	**Analytics of Viber Activity**	data for the purpose of improving our services, and for example: ● We use activity data, device identifiers, IP-based location, user feedback you choose to provide or communications to us and, with your permission, GPS based location, 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 further rely on legitimate interest when Viber (and not a third-party) processes this data for the purpose of customizing and personalizing the Services, for example we use your data provided through registration, or your activity data, and inferred gender, age range, or inferred interests and general location (and, with your permission, GPS based location) to customize content we show you, including our customized offers of certain services. When we use third-party data, or information not obtained through the use of the Viber App or Services, we will seek your consent as further detailed below. When we advertise our Services to you on third party platforms, we may 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 and

• Inferred interests; • Inferences from third party data and ads-related interactions. ● Data we collect from your communications with us, including support, customer services and other inquiries.		further to look for similar users. Additional information (including how to opt-out of data collection through the use of cookies) is available on our **Viber Ads, Cookies & Tracking Technologies Policy** and under your choices and controls explained in **Your Rights Related to Your Personal Data** section below.
Data provided or collected through registration & under your Viber account: ● **Identifiers**, such as: • Your mobile number; • Your personal details; • Your contact details. ● **Dating Data** (excluding any sensitive or Special Categories of Personal Data) Geolocation data: ● **General location** • **City** • **Country of residence** ● **GPS based location**	**Marketing Communications & Location Based Offers**	**Legitimate Interest:** We rely on legitimate interest in connection with our processing of this data, for example: ● Your email address, name, inferred gender, age range, certain dating profile data, device and activity data, for the purpose contacting you with marketing and offers relating to products and services offered by Viber, and our third-party trusted partners. When advertising Viber services outside of Viber, we might share your email address or device identifiers with our trusted marketing vendors. ● Your IP address will be used to extract your general location (city level) or, where provided, your country of residence, for the purposes of presenting offers applicable to your region. Please note that even after you have chosen to unsubscribe (see how you can do it in **Your Rights Related to**

Data we collect automatically from your device: ● **Device identifiers** ● **Electronic network activity data** ● **Activity data** ● **Other device data** Data we collect from other sources and inferred data: ● **Data from publicly available resources and trusted third parties** ● **Social media data** ● **Inferences about your account and Device Identifier:** • Inferred gender.		Your Personal Data section), we may send you service-related communications, including administrative messages that relate to your use of the Services. **Consent:** We will obtain your consent in order to collect and use GPS location data for the purpose of precise location-based marketing offers and communications. You have the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
Data provided or collected through registration & under your Viber account: ● **Identifiers**, such as: • Your mobile number; • Your personal details; • Your contact details;	**Customer Service & Operational Messages**	**Performance of Contract:** We process this data when it is necessary for performing our contract with you, meaning – to communicate with you, give you information about your account, and respond to your requests and inquiries. **Legitimate Interest:** We rely on legitimate interest with our processing of this data for the purpose of improving our customer support (for example in order to train our customer

• Your account login details. ● **Your phone address book** Geolocation data: ● **General location** Financial information provided or collected through your use of our limited financial services (e.g., payment solutions), or purchased subscription and offer. Data we collect automatically from your device: ● **Device identifiers** ● **Electronic network activity data** ● **Activity data** ● **Other device data** Data we collect from other sources and inferred data: ● **Social media data** Data we collect from your communications with us, including support, customer services and other inquiries.		support team, as well as internal management operations).
Data provided or collected through	**Safety, Security & Fraud Prevention**	**Legitimate Interest:**

registration & under your Viber account: ● **Identifiers**, such as: • Your mobile number; • Your personal details; • Your contact details; • Your account login details. ● **Your business accounts data** ● **Dating Data** Geolocation data Financial information provided or collected through your use of our limited financial services (e.g., payment solutions), or purchased subscription and offers: ● **Purchased subscriptions, products or services:** transactions-related information (e.g., the purchasing amount). ● **Viber payment services** Data we collect automatically from your device: ● **Device identifiers**		We rely on legitimate interest in connection with our processing of data for security purposes such as, authentication, identity verification and fraud and spam prevention. This may include URLs included in messages and messages, which were reported as SPAM by other users, or were otherwise suspected to be unsolicited and using your operating system authentication services. We may use automated decisions to close or restrict an account based on such data and other logic we have created for this, in order to protect other users and prevent recurring breaches. We will use some of the information connected with the use of Viber payment services to prevent fraud and ensure security of your wallet account. We may examine the content related to your business account and dating profile to ensure users' safety and prevent fraud. We may use data from trusted third parties related to your IP addresses to enhance the precision in detecting fraudulent activity. When you use our AI features such as AI chatbot assistants, we keep your chatbot communications to ensure your interactions are safe and prevent harm to you or others.

● **Electronic network activity data** ● **Activity data** ● **Other device data** User Submitted Content: • Your chatbot communications, only when you use our AI features. This may include information that could be considered sensitive and personal in nature, if you choose to provide it		
Data provided or collected through registration & under your Viber account: ● **Identifiers, such as:** • Your mobile number country code; • Your personal details, (e.g., name, date of birth), if you provided them ● **Dating Data** (excluding any sensitive or Special Categories of Personal Data)	**Advertising (Placing Third-party ads in the Viber App)**	**Consent:** We obtain your consent in order to use and share certain data, such as device data and device identifiers (i.e. 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 with third party advertising partners for the purpose of personalized advertisements. Additional information (including how to opt-out of data collection through the use of cookies) is available on our **Viber Ads, Cookies & Tracking Technologies Policy**.

Geolocation data: ● **General location** ● **GPS based location** Data we collect automatically from your device: ● **Device identifiers** ● **Activity data** ● **Other device data** Data we collect from other sources and inferred data: ● **Social media data** ● **Inferences about your account and Device identifier**		In addition, we will obtain your consent in order to collect and use your Viber activity data, and information we receive from third parties on your activity outside of Viber, and certain dating profile data, for the purpose of personalized advertising. You have the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. **Legitimate Interest:** We rely on legitimate interest for ad measurements and optimization relating to the performance of ads or campaigns and delivering ads, detecting fraud or for calculating payments. We further rely on legitimate interest for contextual advertisement, meaning, advertisement that is based on country level location and the content you are currently reviewing (for example: a user who is reviewing posts in the explore screen about animals and is from Italy, might be displayed an animal related ad in Italian).
Business partners data	**B2B Communications and Services**	**Performance of Contract**: Our processing of this data might be necessary for performing our contract with you (depending on our engagement). This includes processing identifiers, such as business email addresses and login data for Viber's internal resources (e.g. secure portals and knowledge bases), required to enable the business partners' access

		to Viber business features and APIs, enable account functionality, provide visibility and tracking of account actions (such as template management and deletions), and maintain the security of account activity. **Legitimate Interest:** We rely on legitimate interest in connection with our processing of this data, including for direct marketing purposes – meaning, we will store your email address and use it to send you our marketing offers. You have the ability to opt out of our direct marketing emails at any time. We further rely on our legitimate interest to process business partners data to analyze how our business services are used and to improve our service offering.
Non-User Data	**Provide Service using Non-User Data**	**Legitimate Interest:** We rely on legitimate interest in connection with the processing of non-Viber users' phone numbers and contact names (if provided to us by a user through sharing their contacts or otherwise) for the purpose of showing our user who in their contacts is already using our Services and who is not, to allow the user find and communicate with their contacts who are users in a more efficient way, and to add such contact to the Caller ID database and use as part of Viber Caller ID feature (for more info see

		here), to ensure Viber identifies spam calls outside of Viber for the purpose of reducing spam, fraud and harassment world-wide. **If you are not a Viber user and would like to be excluded from any such processing, please contact us at https://help.viber.com/en/contact. Additional opt-out from the processing as part of the Caller ID service is also available on this page.**
May include all types of data Viber stores, depending on the circumstances, as detailed under **The Data We Collect** section above.	**Defend our Rights & Enforce our Policies**	**Legitimate Interest:** We rely on legitimate interest in connection with our processing, use and sharing of data for the purpose of defending our rights and enforcing our polices, terms and agreements, for example, in the event of a dispute, claims and legal proceedings, and solely to the extent necessary for such purpose. For example – we may record and log some of your actions, such as acceptance of our terms and polices, acceptance of certain offers and notices; we may examine the content and data you upload in relation to your business account or Dating Data to ensure the enforcement of our policies, including per our **Acceptable Use Policy**, **Dating Community Guidelines** and **Viber Business Accounts Terms and Conditions**.
May include all types of data Viber stores, depending on the	**Compliance with Legal Obligations & Public Interests**	**Compliance with a legal obligation;** We use your data where it is necessary to comply with legal obligations to

circumstances, as detailed under **The Data We Collect** section above.		which we are subject to and cooperation with regulators and law enforcement bodies – where there is a valid legal request such as binding order. Please see below examples of EU laws and Luxembourg laws that apply to Viber and according to which we may process, use, maintain or store your data: • **Data Protection Legislation:** We will process your personal data upon your request to exercise your rights under the GDPR. We will store an indication of your access request and order to be able to demonstrate compliance. • **Corporate and Tax Legislation:** We may be required to provide regulators with information under applicable corporate and tax legislations. • **Consumer Protection Legislation:** We will process your personal data in accordance with local laws enacted under Directive EU 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services. • **Telecommunications:** We will process telecommunication data in accordance with local laws enacted under the Eprivacy

		Directive and under the future e-Privacy Regulation. • **Criminal Investigations and Legislation:** We may be required to provide authorities with information in compliance with criminal investigations laws applicable to electronic communications provider or otherwise applicable to us. • **Civil Proceedings:** We may be required to provide authorities with information in compliance with regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters and Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters. **Protection of vital interests:** We may process your data 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.

Back to top

Profiling and Automated Decision-Making

When you use our dating services, we collect and process certain personal data (including gender, interests, location, and other information you provide) to offer personalized match recommendations. This involves profiling and automated decisions. Such automated matchmaking is essential for providing our dating service.

The automated process analyzes user-submitted information and preferences to generate potential matches. These automated decisions enable us to suggest dating profiles of individuals who may be compatible with you. We do not use any dating chat content or data unrelated to dating profile to determine your matches. Note that our matching algorithm is built to follow your configured dating settings hence you can affect the profiles shown to you. You can find detailed information regarding the matching system in our Dating Terms and Conditions.

Further, for safety and moderation, automated tools help detect violations of **Viber's Terms of Service**. We use a combination of automated systems and a team of moderators to monitor and review account.

If you have any questions or wish to exercise your rights related to profiling or automated decision-making (e.g. to request human intervention, or receive an explanation of the decision, please **contact us**.

Back to top

Data Sharing – Categories of Recipients We Share Personal Data With

We share data with third parties, including our corporate family and with trusted companies that help us provide our Services in compliance with strict data security and privacy practices, as well as other third parties such as our advertising partners and third parties offering services through our App. We may also share personal data in limited circumstances where we are required to do so under applicable law. You can find here information about the categories of such third-party recipients, what other Viber users can see, as well as the purpose for which the personal data is shared with such third parties.

Categories of Recipients	Additional Information
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**), and subsidiaries, for the following purposes: • Certain types of data, such as name, email, photo, phone numbers and Viber unique ID, may be disclosed in order to provide joint content and our Services (e.g., registration, coordination of membership accounts between the Viber corporate family, transactions, analytics and customer support).

	• Additionally, we may share certain types of data about you as may be necessary to help detect and prevent potentially illegal acts, violations of Viber policies, fraud and/or data security breaches. • We share data with Viber's subsidiaries due to our global operations, as we have teams and offices located worldwide, and each such subsidiary may operate the services or other functions (e.g. development.) for a certain region. Your Rakuten account or any activity related to your use of Rakuten services is governed by **Rakuten ID Privacy Policy.**
Our Service Providers	We share your personal 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. This includes the following categories of service providers: • **Advertising and marketing service providers**, who help us with advertising measurements and app installations; • **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 improve, personalize, enhance our Services and moderate the content; • **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; • **AI service providers**, which enable AI features on our app, including summary, in-chat assistance and chatbot features; • **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 information with services providers and partners, we ensure they only have access to such information that is strictly necessary in order for us to provide the Services. These parties are required to secure the data they receive and to use the data for pre-agreed purposes only, while ensuring compliance with all applicable data protection regulations (such service providers may use other non-personal data for their own benefit).
Third-Parties Offering Service Through our App	As part of Viber's Services, we allow third parties to create communities, channels and business accounts 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 you, 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 and are considered "independent controllers" of such data for the purposes of the GDPR, meaning, their use of

	your data shall be subject to their policies and privacy practices.
Advertising Partners	We will share with such advertising partners, including partners managing our advertising placements , unique device identifiers (i.e., advertising identifiers associated with your device or identifier that tell your device apart from other users and may be assigned to your device by Viber or our advertising service providers/partners) along with age range, inferred gender, country, city, reduced IP address and certain technical or aggregated data (e.g., your language preference). 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 & Tracking Technologies Policy**. The list of our advertising partners is available **HERE**
Legal and Law Enforcement	We may disclose certain data 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 necessary to comply with such purpose. This disclosure is subject to our strict data security and privacy practices and without compromising our end-to-end encryption. It may include, depending on the circumstances, certain types of your Activity Data, Identifiers and phone address book.
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 our Privacy Policy (including this notice), and we will notify you of such corporate changes in your data processing.
Limited Payment Services	If you use our Viber payment services, we will share with our payment service providers KYC data, fraud data, payment requests/ instructions, specifically requested information (i.e. due to a specific issue), transaction and wallet related information. If you use our Viber Chatbot Payment, we will share with Google Pay or Apple Pay or any other linked payments provider the following information: (i) name of the Payment Service Provider merchant; (ii) price of the items purchased and currency; and (iii) the description of the items purchased. 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**. If you use our Viber Out Credit, paid features or purchase Premium Services' subscriptions, and such purchase was made not through app stores, we will share your email address with our payment processor, for the purpose of verification and fraud detection.
Other Users	When you use our Services, other users can see certain data about you: ● Unless you have changed your settings: • your user name and photo;

	• your phone number (if you are in communication with them or have a business account); • your connection status; • whether you have received and seen messages sent to you. ● If you are currently on another call. ● If they are part of the call with you, data related to the calls and messages you have sent and received such as length of the call, who called who, who messaged who, and at what time, the type of call (audio/video) and whether you answered the call on your primary or another device. ● For disappearing messages, we will notify the other users of any screenshots you've taken (so please respect the vibe and do not take them). ● Your name and photo may be shown to users who turned on the Viber Caller ID feature when you initiate a phone call with them (on Viber or mobile). ● When you join Viber, the contacts in your address book that are already Viber members may be informed that you're now on Viber too. ● A reminder about your birthday on the date of your birthday unless you have changed your settings. ● When you join Viber payment services, the contacts in your address book that are already Viber members may be informed that you're now using Viber payment services. In addition, Viber users will see an indication whether you are a Viber payment services user and perform in app transactions with you. ● When you send money using Viber payment services, the recipient can see transaction and other related information including the IBAN, swift code, sort code, account number, amount, time, payment reference and for group payments the purpose and payment status of others in the group. The sender will see certain letters of the first and last name of the

	recipient, if the recipient of the transaction is not in the sender's address book, so that the sender may verify that the recipient is a correct beneficiary of the transaction. ● When using the dating services, the information included in your dating profile as well as any other content you choose to share, may be presented to other participants of the dating services. VIBER STRONGLY ENCOURAGES YOU TO USE CAUTION IN DISCLOSING ANY PERSONAL INFORMATION ONLINE INCLUDING THROUGH YOUR DATING PROFILE. ● If your "Use Peer-to-Peer" option is on, other users can use technical tools to see your IP address. You can turn this option off at any time on your privacy settings. ● **Your public posts:** If you post information on our public spaces such as communities, channels, business accounts, dating profiles, it may be searchable and available to other users on Viber. You can always delete your posts on those public spaces, but Viber cannot control and is not responsible for what other users do with this information (e.g., store on their devices, publish on Viber or outside of it etc.), thus, we recommend you do not disclose your personal data through the content of your posts. ● Quality indicators and tags on your business account (e.g. responsiveness and activity indicators, categories) or dating profile (e.g. activity indicators) assigned by Viber, which are intended to provide other users more meaningful information about your business account or dating profile.

Back to top

Data Transfer

Due to our global operations, your personal data will be shared with Viber corporate family, as well as our service providers and business partners around the world including outside the EEA and UK. We take measures to ensure the transfer of such data will provide sufficient safeguards, as required under the GDPR. These measures include compliance with Binding Corporate Rules of the Rakuten Group, as well as contractual

commitments of our partners and service providers. We further explain below why we transfer personal data, the measures we take to ensure your personal data will be secure upon transfer, and your rights in this regard.

Due to our global nature and operation, your personal data may need to be processed in countries that may not offer the same level of protection as in your home country. When personal data collected within the EEA and the UK is transferred outside these locations, we will take the steps necessary to ensure that the transfer of such data provides sufficient safeguards, as required under the GDPR.

- We store and process all categories of your personal data on our computers and servers. Your data will be stored in our servers located in the US, however note that, our communications servers are located globally in order to enable the operation of our communications services.
- As part of the Rakuten Group, the transfer of your personal data to entities which are a part of our Viber corporate family (whether located in the EEA and UK or not), are made in accordance with the Rakuten Group Binding Corporate Rules to legitimize international data transfers within the Group. The Rakuten Group Binding Corporate Rules can be found at **https://corp.rakuten.co.jp/privacy/en/bcr.html**
- Some of our service providers and business partners are located in various locations, including outside of the EU, EEA or UK. In such events, transfers of your personal data will be made in accordance with applicable data protection laws, and as specifically, without derogating from the above, all transfers of personal data outside the EU, EEA or UK are also subject to the provisions of the Standard Contractual Clauses (known as "**SCC**") approved by the European Commission (and the equivalent for the UK and for Switzerland where applicable) available **HERE**. Where applicable and required by law we ensure supplementary measures are placed, such as encryption in transfer and at rest.

Subject to applicable laws, you may exercise your rights to receive information on such transfer mechanisms detailed above, by contacting us through **our online form available at: https://vb.me/ContactUs** (please choose the "privacy inquiry" or "GDPR inquiry" categories), or through additional means of communications we have provided under this notice.

Back to top

Data Retention

As we have explained above, we process personal data for various purposes. Accordingly, we only keep personal data as long as required to fulfill the purpose for which the data was collected, or, in some instance, where we have other necessities to

retain the personal data, for example, where required by law. We explain below the criteria used by us to determine the retention of your personal data (meaning, for how long we store it and when we delete it, aligned with the type of data and purpose of collection).

The criteria used by us to determine Viber's retention periods are as follows:

- **The type of personal data and purpose of collection –** unless otherwise specified, we retain data as long as it is necessary and relevant for us to achieve the purposes for which the personal data was collected. For example:
    - Personal data required to be retained in order to maintain your Viber account and to enable you the use of Viber Services – these types of data, including your mobile number, and phone address book, will be retained for as long as you maintain your Viber account.
    - Personal data you have voluntarily provided during registration or through your account (including dating profile or business account data) – these types of data, including your photo, date of birth, email address, will be retained for as long as you maintain your account.
    - The details of your communication with our customer support team will be stored for 10 years.
    - Call Detail Records of your free Viber calls and messaging activity, as well as records of your in-app activities (jointly, CDRs) are kept as a raw data for 24 months from creation. CDRs may include, for example, you phone number and device identifiers (i.e., IP address, unique device identifier).
    - We delete any message once delivered, or after 14 days if delivery attempts throughout this period was not successful.

If you decide to delete your Viber account, the CDRs and communications with our customer support will be retained as detailed above, and we will further retain records of financial information with respect to Viber payment services this means KYC data, transaction and wallet related information or your hashed pin code), Viber Out usage including CDRs, purchasing subscriptions for the periods required under applicable laws, or as needed in accordance with our fraud monitoring program or to identify a returning user (for Viber payment services).

All other types of data related to your Viber account will be deleted, unless we are required to further retain the data, subject to the criteria detailed below. We may keep measurement data and activity data on a non-identifiable basis to improve our Services and for business analytics purposes. Your posts on channels and communities may remain available if you do not delete them. Please note that deletion of the App (i.e., uninstall the App from your device) will not immediately delete your account, but if you

do not reinstall it within subsequent two weeks your account may be deactivated; provided however if you have Viber Credit under your Viber Out account, other time periods will apply as set forth under "Viber Credits Specifications" clause of Viber Out Service Specific Terms and any eSIMs purchased through the App will remain active on your device independently of the App. Note that your account may also be deactivated if you do not log into Viber for twelve consecutive months. Please see information and instruction regarding your account deletion **HERE.**

- **Compliance with our legal obligations** – we are required to retain certain types of data in order to comply with our obligations under applicable laws. For example, we need to retain transactions information to comply with tax legislation. In addition, we may retain certain types of personal data in the event we are required to do so subject to a binding legal request or a court order. Further, subject to EU Directive 2002/58/EC we are required to retain certain personal data (such as phone number) to convey messages and calls.
- **Dispute, claims and legal proceedings** – if you have a dispute with us, we may retain certain types of personal data as necessary and applicable to your claims, including any legal proceedings between us, until such dispute was resolved, and following, if we find it necessary, in accordance with applicable statutory limitation periods. In addition**,** in the event you request to exercise your rights, we will maintain the applicable correspondence for as long as needed to demonstrate compliance, and usually in accordance with applicable statutory limitation periods.
- **Retention for Non-Users' Data** – if you are not a Viber user, and we process your data to enable Viber users to communicate with you via Viber Services, we will retain such data as long as it is relevant to Viber users, or until you have requested us to stop processing your phone number. You can request to exclude your phone number and opt out **here**. You can also opt out from the processing under Viber Caller ID service by contacting us **here**. Furthermore, if one of our users used our Viber Out Services in order to communicate with you (i.e., call you through Viber), we will retain a log of such call (Call Detail Records – CDR – as detailed above), which will include your phone number, for 24 months from creation. In relation to Viber payment services we store non-user data as long as it is relevant to a Viber payment services user (i.e. you are the sender or a recipient in a transaction with them or as part of a promotion). Further, this information may be stored as part of our fraud prevention program or in response to specific customer queries.

Back to top

Your Rights Related to Your Personal Data

Under the GDPR, you have certain rights regarding the personal data that Viber has collected about you. Such rights may include (depending on the type of data and our lawful basis for processing) the right to know which types of data we collect and why we collect it (as we detail under this notice), the right to request rectification of your personal data, the right to request us to delete your personal data, the right to restrict processing of personal data, the right to data portability, the right to access your personal data, the right to object to the processing of certain forms of data, the right to appeal automated decisions and profiling, the right to withdraw your consent at any time, as well as the right to lodge a complaint to a supervisory authority. We further explain below the operational meaning of each such right, as well as when and how you may exercise your right.

The Right to Be Informed

This EU Region Privacy Notice and **Viber's Privacy Policy** describes our practices in detail using simple language. Everything you need to know is here. If you have more questions, feel free to contact our **support team**.

The Right to Rectification

If you believe we have the wrong data about you, or that your data is incomplete, feel free to change it at any time through the profile settings on your Viber settings on your mobile device. You may edit your dating profile data at any time through the dating profile (except for such non-editable categories as your name, age and gender). If you can't find what you are looking for, **contact us**.

The Right to Erasure

You can exercise your right to erasure in the following ways:

- **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 activity logs, as described in our Data Retention section).

If you use specific Viber services that maintain a separate profile (such as Viber Dating or 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. For example, you may delete your Dating profile through the Dating Settings in the App or your Business Account through the Business Account settings. Deleting a service-specific profile removes the data associated with that service.

- **Delete your data while continuing to use the App.** We have also 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. And no need to worry – deleting your data won't remove the chats on your Viber App on your phone and allowing the continued use of the App. Please note that content shared, sent or made available to other participants of the dating services prior to your account deletion may be retained and utilized by such participants, outside of our control and responsibility. For a full description of what is and is not deleted through each method, check our support articles **here** and **here**.

The Right to Restrict Processing

We allow you to opt out of certain processing of your data by using the **Viber privacy settings** on your mobile device. You can decide which processing operations you want to opt-out of. You can also change the settings on your mobile device operating system at any time to prevent us gaining access to certain data such as your accurate location – but this may negatively impact on your user experience.

The Right to Data Portability

We have created a **request your data button** in Viber's privacy settings on your mobile device to make a simple way for you to access the data connected to your account. Once it is ready, you will receive a file from Viber containing this data.

The Right of Access

You may access your data by using the **request your data button** and for further access requests you can contact our **support team.** If you have further questions **contact us.**

The Right to Object (Right to Opt Out)

You can object to the processing of certain forms of data by contacting our support. Complete this **online form** and explain your special circumstances. If you receive emails from us, you can always opt out on the bottom of the email, or by contacting our support. We also allow you to opt out of certain processing of your data by using the **Viber privacy settings** on your mobile device.

The Right to Contest Automated Decisions and Profiling

We may make an automated decision to block a user, in case we suspect this user is using our services for illegal acts or acts that violate our terms of service. If you believe that your account was unlawfully blocked, you can contact our **support team**. Please

note that as explained above, certain features of our Services, such as the dating services, may inherently involve Automated Decisions and Profiling.

The Right to Withdraw Consent

Where we have collected or other process your personal data based on your consent, at any time, you have the right withdraw your consent. However, please note that withdrawing consent may limit or prevent your use of certain Services, such as our Dating Services, inherently necessitating the processing of certain Special Categories of Personal Data.

If you would like to further understand or exercise your rights, please contact us by:

- **Our online form available at: https://vb.me/ContactUs** - please choose the "privacy inquiry" or "GDPR inquiry" categories.
- **Using the "contact us" form on the App**.
- **Email**: **DPO@viber.com**
- **By mail:**
  Viber Media S.à r.l.,
  Attention: Data Privacy Officer
  2, rue du Fossé, L-1536
  Luxembourg, Grand Duchy of Luxembourg.

We will contact you if we need additional information from you in order to honor your requests.

You have the right to submit a complaint with our lead supervisory authority or any other competent data protection supervisory authority. Our lead supervisory authority is the National Commission for Data Protection – Grand-Duchy of Luxembourg. If you are located in the UK, you may also submit a complaint to the Information Commissioner's Office (ICO). **Before submitting a complaint, we always encourage you to contact us first using the methods above so we can address your concerns directly.**

In addition to the above, Viber provides you with certain choices and controls you may exercise, related to your personal data, as follows:

- We enable you to delete or edit 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 are available within the App.
- You can also make additional choices on your phone's settings by changing our App's permissions such as GPS location sharing, access to contact list and more.
- You can choose not to display your Viber payment services badge.
- 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, 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 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.
- You have even more choices (such as use Viber with no ads, invisible mode, deleting messages without a trace) under our premium Viber Plus service.

Back to top

Children's Privacy

Our Services are not intended for children under the age of 13 and we do not knowingly collect personal data from individuals under this age.

Our Services are not intended for children under the age of 13. Therefore, we do not knowingly collect personal data via our websites, applications, services, or tools from anyone under 13. If we have actual knowledge that you are under the age of 13 (or the minimum age at which a person may use the Services in your state, province, or country without parental consent, if greater), we will stop providing Services to you and delete your account and data. In the EEA and the UK, certain default privacy settings will be applied to children. Learn more about the age restrictions on Viber **here**.

Some of our features, like business accounts and Dating Services are strictly limited to users over 18, and we retain our right to request any additional data from the user for validating its eligibility to use such services.

Changes to this EU Region Privacy Notice

We may make changes to this EU Region Privacy Notice from time to time. If we do (except for minor tweaks), we will notify you via our App and website.

We may modify or update this privacy notice from time to time.

If we change this privacy notice (except for technical tweaks), we will notify you of the changes. Where changes to this privacy notice will have a fundamental impact on the nature of the processing or otherwise have a substantial impact on you, we will give you sufficient advance notice so that you have the opportunity to exercise your rights (e.g., to object to the processing). The last modification date of this privacy policy will be reflected in the “Last Updated” header above.

In the event you read this policy in any language other than English, you agree that in the event of any discrepancies, the English version shall prevail.

Back to top

Current Privacy Notice for EEA and UK users under the GDPR PDF Version March 2026

Previous Privacy Notice for EEA and UK users under the GDPR PDF Version September 2025