

Last Modified: August 2021

Thank you for using Wickr Me! Wickr allows you to encrypt and send audio, video, voice, text messages and files, and conduct voice calls, so that you can communicate safely, securely, anonymously — and easily.

This document, our Privacy Policy, governs how Wickr (“we”, “us”, “Wickr”) handles our users’ (“you,” “your,” etc.) data both in the Wickr Me app itself (the “Wickr Me App” or “Wickr Me”) and on our website/servers (collectively, the “Services”). This policy does not cover Wickr business products.

Our Privacy Policy is incorporated into and is subject to the Wickr Terms of Service, so please read both documents carefully. Your use of the Services indicates your consent to this Privacy Policy and our Terms of Service. If you do not want to be bound by these agreements, you may not use our Services.

We work very hard to preserve your privacy and security, and we do our best to be as transparent as possible in explaining how we use your data in providing our Services. Not only is Wickr’s security architecture and proprietary encryption methodology designed to ensure that only users can gain access to their message content, we promise to never monetize your communications or personal information. Ever. Please contact us if you have any questions at [privacy@wickr.com](mailto:privacy@wickr.com)

### **Our Privacy Practices in Brief:**

Wickr has to collect some information from you in order to provide our Services to you, but we work to do so in a limited and secure way, as follows:

- We can’t see the messages you transmit using the Service, the rooms you create or your contacts. Because of this we don’t know — and can’t reveal to others — anything about you or how you use the Wickr Me App aside from the limited information such as the date your account was created, the date of last use and the type of device on which such account was installed. Please see our [Legal Process Guidelines](#) for more details.
- We do not track, log or store users’ unique device information, IP or geo-location data or similar metadata associated with your use of the Wickr Me App.
- When you send or receive files using Wickr Me, it is important to note that if you do not trust the person you’re talking to, do not open files coming from them or send them photos/files you do not want to be saved.
- You control how long your messages are viewable on recipient devices. However, there is no magic pill for betrayal and we cannot prevent someone using a camera to take a picture of a message on a screen. Therefore, we strongly encourage you to only send private messages or sensitive information to people you know and trust.
- When you block someone from being able to contact you on Wickr Me, they are automatically added to the block list in your settings. To protect your privacy, they won’t know that you are blocking them when they send you a message.

- If you enabled message notifications for Wickr Me, you will receive notifications about incoming messages on your device's home screen which will contain the sender's name as you set it in your Wickr contacts. You can also enable message preview in Wickr settings for notifications, which will add the content of a message to the home screen notifications. Please note, if you don't want other to see who is messaging you on Wickr Me, you can disable notifications in your device settings in which case you will continue to receive messages, but notifications will not appear on your home screen.
- You own your data. We do not share or sell any data about our users. Period.

### **What Information Does Wickr Collect and How Is It Used?**

We are committed to limiting our collection of your information to what is necessary to provide you with our Services in accordance with applicable data protection and privacy laws.

The limited information we collect, receive, or have access to is used to provide the Service, to allow you to send and receive messages and files, to respond to your requests, and to improve the Service, in line with the legitimate interest we have in delivering the Services to you. It may also be shared under valid legal process and with third party service providers for the limited purposes described below.

### **What We Don't Collect**

Equally important to us is to share what information we don't collect. We do not collect your location information or have access to the contents of the communications you send using the Wickr Me App. Remember, however, that if you send a Wickr message to another Wickr user, that message or related content might remain on their device even after you delete it from yours, depending on the value you set for the expiration or burn-on-read time of that message and whether the recipient took a screenshot of the message.

### **User-Provided Information**

We collect some very limited information from you after you download the Wickr Me App in order to allow you to create a Wickr Me Account, and begin using the Wickr Me App.

- **Your Wickr ID:** Your Wickr ID is how you allow others to contact you via Wickr Me. It does not have to be your real name or provide any reference to your identity. Like other information pertaining to your account, it is disguised with multiple rounds of salted, cryptographic hashing when we associate it with your Device Information (described below). The purpose of using this hashed representation is to allow you to use our Services without our needing to know who you are.
- **Your Password:** We require you to have a password to use the Wickr Me App, but we never store your password on our servers and don't store it by default in any form on your device. For your own security, we recommend that you use a long, unique password consisting of a mix of upper- and lower-case letters, numbers, and symbols.

### **Optional User-Provided Information**

Within the Wickr Me App, we provide a few optional features for your convenience. Some of these features, described below, will ask for personal information. If you want to keep your use

of Wickr Me as anonymous as possible, please read these sections carefully in order to understand how we associate information you provide with your Wickr Me account.

- **Push Notifications:** When setting up your Wickr Me account, we will ask if you want to receive notifications of new Wickr messages, software updates, and other administrative and technological developments. Push notifications are functions of device's operating system, so if you enable this feature, your devices operating system's manufacturer will know that you are using the Wickr Me App, but will not know anything about how you use it or be able to see anything you transmit through it.
- **Phone Number:** If you add your phone number to your account to facilitate contact searching, we use a third party service to deliver a confirmation SMS to you, but that service will not receive any information about you other than your phone number, and the SMS message itself will contain no information except a confirmation link. We then store a hashed representation of your phone number on our servers in lieu of the actual phone number to facilitate searching. Our contact search feature operates entirely on hashed representations of phone numbers and rate limited search functions.
- **Invitations:** If you wish to invite others to use the Wickr Me App, you will be asked for permission to access your device's contacts in order to invite them to use our Services. We never store your device contacts on our servers in any way. All invitations are generated locally on your device, without sharing any information with us.
- **Contacts:** If you allow the Service to access your device's contacts to see who among them is on Wickr Me, the Service will send hashed representations of your contacts' phone numbers to our servers to ensure that our server never accesses your actual contact list. We never store your device contacts in any form on our servers.
- **Avatar:** If you set a public profile avatar, it will become visible to others on Wickr, so please do not add an avatar if you do not intend it to be viewed by other users.

### **Automatically Collected Information**

Wickr collects two types of information automatically during your setup and use of the Wickr Me App: Device Information, Aggregate Usage Data, and Crash Logs.

- **Device Information:** The Wickr App may collect hashed representations of your mobile device's hardware ID and/or other platform-related information during registration. This information is used to tie your account to your device.
- **Aggregate Usage Data:** During the operation of our services, we also collect aggregate, anonymous information about basic usage statistics, such as the number of messages sent by Wickr Me users daily, what types of messages our users tend to send (e.g., voice messages more often than text), and other key performance indicators. We never attempt to, and cannot, identify users associated with any of this information.
- **Crash Logs:** For the purpose of debugging, error correction, and system continuity, Wickr Apps transmit crash logs to a cloud-based bug reporting platform. The logs do not contain any user personal information and they pertain only to the Wickr Me App.

### **What Information Does Wickr Share with Third Parties?**

We do not share any user information we have with third parties, with the exception of the third-

party service with whom we share your phone number for the sole purpose of sending you an SMS confirmation if you choose to associate your phone number with your Wickr Me ID.

**Law Enforcement:**

Please see our full [Legal Process Guidelines](#), but here are the highlights:

We will always notify our users of any third-party requests for their information unless we are legally prohibited from doing so. As soon as legally permissible, we will notify our users of requests for their information. We require a warrant before handing over the contents of communications; however, because of the nature of our technology, the contents of communications will be encrypted and undecipherable if obtained.

**You Can Terminate Your Account**

You can terminate your account at any time. Once terminated, your account will be irrevocably suspended, ensuring that nobody can use that Wickr ID again in order to prevent impersonation. If you wish to terminate your Wickr Me account, go to Settings, “Terminate Account” and verify by entering your password.

**We Retain As Little Data As Possible, for the Least Time Possible**

**Data Retention on Wickr’s Servers:** Our servers store the encrypted messages that you send and receive for up to 6 days to ensure their reliable delivery to each device associated with your account and the accounts to which you transmit messages. We retain certain account data (i.e., types of messages sent and account settings changes) which contain no PII for up to 6 days.

**Data Retention on Your Device:** All messages are stored in encrypted form on end users’ devices. You choose your own retention policy for your messages by choosing how long a message is viewable before it is deleted (via the expiration or burn-on-read time for sent messages, recall ability and manual deletion for your device). In addition, Wickr’s [“secure shredder”](#) technology uses forensic deletion techniques to help reduce the risk of deleted messages and temporary data being recovered.

**We Are Serious About Security**

We are concerned about safeguarding the confidentiality of your information. We provide physical, electronic, and procedural safeguards to protect information we process and maintain. For example, we limit access to this information to authorized employees who need to know that information in order to operate, develop, or improve our Services. No sensitive information is in the clear: we take reasonable efforts (as described herein) to ensure that everything we store is not retrievable by us or anyone else.

However, as security experts, we know that no security system can prevent all potential security breaches. Therefore, we have limited the potential implications of such a breach by designing our system so that in the event of a breach, we would have the least possible information about you.

Wickr's network infrastructure and services are maintained in highly secure, strategically located data centers managed by Amazon Web Services (AWS). Learn more about AWS security policies [here](#).

### **Children**

Wickr is not directed to children under the age of 13. If we learn that we have allowed a child under 13 to access our Services, we will take appropriate steps to promptly remove such account and delete all information associated with such account.

If you live in any other country except those in the European Region, you must be at least 13 years old to register for the Services. If you live in the European Region, you must be at least 16 years old to register for and use our Services.

### **Customer Service**

In an ongoing effort to improve our services and assist our customers with any questions they have about the use of the Wickr Me App, we have developed a comprehensive collection of the most commonly asked customer support questions and answers, which are available [here](#). Any information provided to us by our users voluntarily when they request customer support (e.g., an email address, Wickr Me App version, or any other details related to user issue) will be used to respond to that individual request and may be logged as part of our effort to improve our customer service and solve any product-related issues. This user-provided information cannot be linked to our users Wickr Me accounts, unless users voluntarily include their Wickr Me account information in their customer service-related requests. We strongly discourage our users from disclosing their passwords to Wickr Me accounts to third parties.

### **Cookie Policy**

We tirelessly work on improving our services and raising awareness about our products, which are designed to ensure our users' security and privacy. To accomplish these goals, we use cookies on the Wickr website that enable us to learn how visitors navigate our content and interact with our marketing materials so we can be more effective at informing our users about product developments.

A cookie is a small text file that is placed in visitors' browsers to help us learn when users arrive at our site, how they use the site, when they leave, and when they come back. These cookies can never be used to identify user accounts within the Wickr App.

Here is an example of how we may use information collected via cookies: we may think that one of our new features would be very useful to the Wickr community, but cookies may tell us that very few users fully read that feature's description on our site. That insight would help us to rethink the way we explain that product on our site or present it in an advertisement so that we can better communicate our services to our users.

We make every reasonable effort to minimize the information we collect. For example, we enforce IP masking for the website analytics purposes to conceal the last 4 digits of IP addresses which ensures that visitor's full IP addresses are not collected via third party services such as Google Analytics.

We provide the utmost transparency on and an up-to-date overview of cookies used on our website including the ability for website visitors to [check, withdraw or modify](#) consent for non-necessary cookies at any time. More information on our Cookie Policy can be found [here](#).

### **Web Forms**

To enable our visitors to reach out to us with sales inquiries, we may collect information using online form submissions. Please note that all information you provide via web forms on our site is strictly voluntary and will never be used in any way that is inconsistent with other provisions of this Privacy Policy.

### **Third Parties**

To improve Wickr's products, website, or marketing, we may engage with various outside partners that have access to the limited data users voluntarily share with Wickr via the app, web forms, cookies, or customer support and sales inquiries. We carefully select each of our partners based on Wickr's commitment to user privacy and security. Our security team meticulously vets each prospective partner to ensure its policies and practices are on par with Wickr's standards.

- To assist Wickr with improving our web content and advertising activities, we partner with [Pardot](#), a B2B Marketing Automation Platform, and [Salesforce](#).
- To accelerate resolution of the most frequent customer inquiries, Wickr's support is automated in collaboration with [Zendesk](#), a customer support platform.
- To deliver a confirmation SMS to our users opting in to connect with friends via ID Connect, we use [Twilio](#).
- To maintain high-security, fast and reliable service delivery worldwide, Wickr partners with [AWS](#), a global infrastructure provider.
- To manage bug reports, we use [Bugsnap](#) and [Backtrace](#), which are cloud-based bug reporting platforms.

Each of these companies has its own policies for handling user data. Please review the respective privacy policies for [Zendesk](#), [Twilio](#), [Pardot](#), [AWS](#), [Bugsnap](#), and [Backtrace](#) for a more complete understanding of their practices.

If you have additional questions regarding our privacy protection practices, please email us at [privacy@wickr.com](mailto:privacy@wickr.com).

---

### **We Can Change This Privacy Policy**

This Privacy Policy may be updated from time to time, for any reason. We will notify you of any changes to our Privacy Policy by posting the new Privacy Policy here along with information about what has changed and an archive of past policies. You are advised to consult this Privacy Policy regularly for any changes. By continuing to use the Services, you agree to be bound by the revised Privacy Policy.

### **Users Outside the US**

If you use our Services, your information will be transferred to the U.S. and will be processed

and stored under U.S. data protection and privacy regulations which may differ from those your country of residence. By using our Services and providing information to us, you consent to such transfer to and processing in the U.S. We take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this policy. Please note that all user communications on the Wickr Service are protected between devices and are never stored unencrypted hence are undecipherable to Wickr or other third parties.

You are responsible for complying with any laws or regulations in your country that govern use of applications and services like Wickr Me.

### **Contact Us if You Have Questions or Account-Related Requests**

If you have any questions regarding privacy while using our Services, or have questions about our practices, please contact us via email at [privacy@wickr.com](mailto:privacy@wickr.com).

If you live in the European Region, please note the following:

**Opt-out.** You may contact us anytime to opt-out of:

- direct marketing communications or
- the transfer of your personal data outside the European Region. Please note that your use of some of the Service may be affected by your opt-out.

**Access.** You may access the data we hold about you at any time within the application or by contacting us directly.

**Amend.** You can also contact us to update or correct any inaccuracies in your personal data.

**Erase and forget.** In certain situations, for example, when the data we hold about you is no longer relevant or is incorrect, you can request that we erase your data. Please note that only you can delete your Wickr Me account at any time from within the Service, due to privacy design of the Service, we are unable to delete Wickr Me accounts upon your request.

You may contact us at [gdpr@wickr.com](mailto:gdpr@wickr.com) on any questions you may have about your personal data and our use of such personal data under the GDPR.