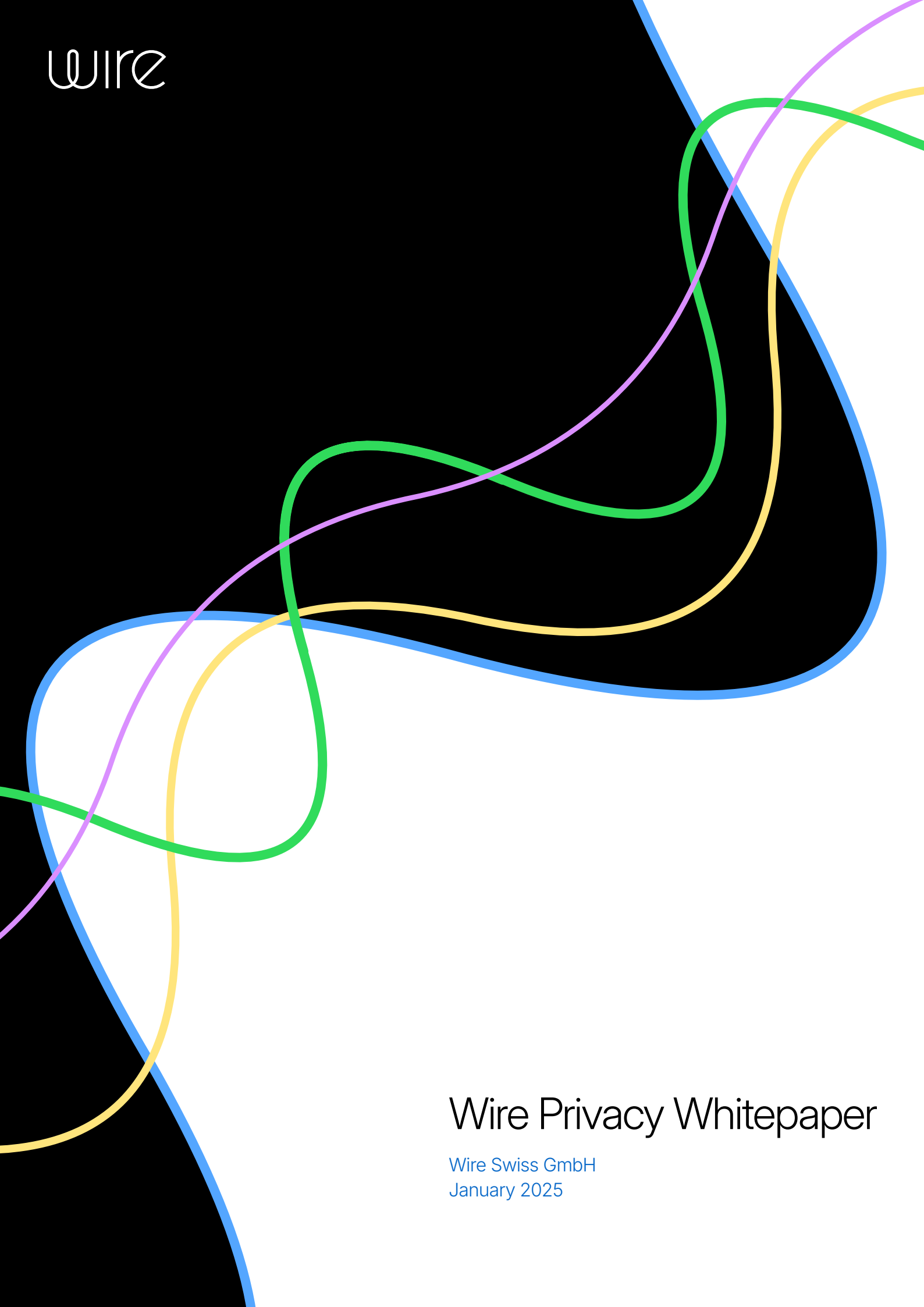


Wire Privacy Whitepaper

Wire Swiss GmbH
January 2025

Introduction

At Wire, we prioritize privacy and believe that transparency and trust are the foundation of strong user relationships. All communication through Wire is end-to-end encrypted – messages, conference calls, and files. Each message is encrypted with a new key. No one, except the participants in a conversation can decrypt information. Wire's encryption works transparently in the background and doesn't need to be activated – it's always on.

This whitepaper outlines Wire's data protection and security principles, demonstrating our commitment to safeguarding user information. It provides a comprehensive overview of the types of data and metadata collected through Wire's applications, detailing how this information is used to enable Wire's functionalities while ensuring the privacy our users expect. If you are interested to read more in-depth about Wire's Security and Encryption, have a look at the Security Whitepaper.

Data protection and data security at a glance

Made in Europe:

- Wire is a Swiss company which means that Swiss data protection laws apply
- Foreign authorities must request legal assistance via Swiss authorities, following the Swiss Federal Act on International Mutual Assistance in Criminal Matters
- All customer data is stored on servers located in Europe

Data protection principles:

- Wire's services are developed according to the principle of "privacy by design" - including privacy in the design phase, right from the beginning
- We only collect the personal data necessary to operate and deliver our services
- Personal data is processed solely for the purposes described in our Privacy Policy
- To safeguard our customer's data, we have implemented extensive technical and organizational measures
- All our employees and external consultants are contractually bound to confidentiality

Data processing

The following section provides a detailed overview of all data that is stored and processed to deliver Wire's services.

Users

Profiles

Every registered user has an associated profile that contains the data that was provided during registration or that was subsequently edited:

- **Username and display name:** chosen by the user
- **UUID:** randomly generated string to uniquely identify the user
- Email used to register
- Profile picture, including metadata, a unique ID, dimensions, and a tag
- Accent color
- **Locale:** An IETF language tag representing the user's preferred language
- **Cookie Label:** A label to associate with the user token that is returned as an HTTP cookie upon successful registration

Wire for Enterprise:

- Additional profile information that may be added to the profile via the SCIM integration

User devices

The following data will also be collected when a new device is enrolled:

- **Class:** The device class: Mobile, Tablet or Desktop
- **Model:** The device model, e.g. iPhone 15
- **Label:** A human-readable label for the user to distinguish devices of the same class and model
- **Cookie label:** A cookie label links the device to authentication cookies (see Security Whitepaper)
- **Timestamp:** The UTC timestamp when the device was registered
- Last active timestamp, rounded to the next multiple of a week (necessary for the encryption protocol migration)
- **Type:** permanent/temporary

Connections
A registered user with a verified identity can establish connections to other registered users.

Connections are established when one user sends a connection request to another and that request is accepted. A private 1:1 conversation is established between the two users in which they can communicate.

Team users automatically have a connection established by default.

A user can block a connection at any time, after which further messages or calls from the blocked user will not be received. Furthermore, a user can not be added to a conversation by someone they blocked. The blocked user is not actively notified that they have been blocked. Team users cannot block connections from people within their team.

People search
People search can be used to find other Wire users. A user can search for contacts by name or by username. The search results for users with whom no connection has been established yet include their display name, username, and profile picture. The way how team users can be searched from outside their team is configurable; for example, they may only be discoverable by their exact username.

Conversations

Conversations are separated from each other, and a user must be part of a conversation to receive content.

Membership
Wire distinguishes two types of conversations:

1:1 conversations which are created implicitly as a result of a connection between two users. No new participants can join or be added to the conversation.

Group conversations. Administrators of a group can add other users that they are connected to (i.e. a user cannot be added to a conversation by someone whom he blocked). Every participant of a group conversation, including the creator, is free to leave the conversation at any time.

Group administrators can allow guests to join the conversation. This is done by inviting guests through a specific link for a certain group conversation. Guests don't have an account, they can also join for longer when logged in with that account.

Team administrators have the option to allow or disable whether guests can be invited to group conversations.

Group data
Wire maintains the following group data about conversations on the backend servers:

- → **Creator:** The user who created the conversation
- → **Timestamp:** The UTC timestamp when the conversation was created
- → **Participants list:** The list of users who are participants of that conversation and their devices. This information is used by clients to display participants of the group and to perform end-to-end encryption between clients (see the Wire Security Whitepaper for further details)
- → **Conversation name:** Every admin can name or rename a group conversation
- → **Role:** Users can have different roles within a group: Group admin, group member (for Wire for Enterprise also guest)
- → The above data is encrypted using transport encryption between the clients and the server

Folders
Wire conversations can be organized into user defined folders. Wire maintains the list of folders and the list of conversations in them. The folder names and the associated conversations are stored in plaintext on the backend to synchronize folders across all clients.

Telemetry

Wire client applications can collect telemetry data with the aim of improving future versions of Wire based on user needs. Telemetry data helps Wire's Product Team to assess how Wire is used and to identify areas of improvement. Telemetry data is not tied to any other user data or shared with third parties and is stored on a dedicated instance separated from Wire's server.

Telemetry data aggregates various metrics of the application's usage, such as whether and when an error occurs or a particular function is used (so-called events).

Client applications will not collect usage metrics if:
- The app is configured to connect to a custom backend rather than the Wire cloud backend
- You are using the Android F-Droid app

User consent
Telemetry data collection is an opt-in feature, giving users the choice of whether or not to participate. Users can opt out or revoke their consent to process product analytics at any time, with changes taking immediate effect for future data collection.

Wire for Enterprise:
Within the Team Admin Panel, the team administrator can configure the team user consent as follows:
- All team admins have the choice to opt-in/out of the data collection of their usage of the Team Management platform
- By default, team management data collection will be opted out. 3.3.2 Product analytics via Countly

Product analytics via Countly
To collect telemetry data, Wire uses the Countly framework (see https://count.ly) while the data is stored on a Countly server instance that is hosted by Wire. After consent has been given, a unique and random analytics ID is generated on the device. This ID is not tied to any user-specific information and never sent to the Wire-messaging backend. The telemetry data is kept segregated from the user ID as the random Countly identifier is used.

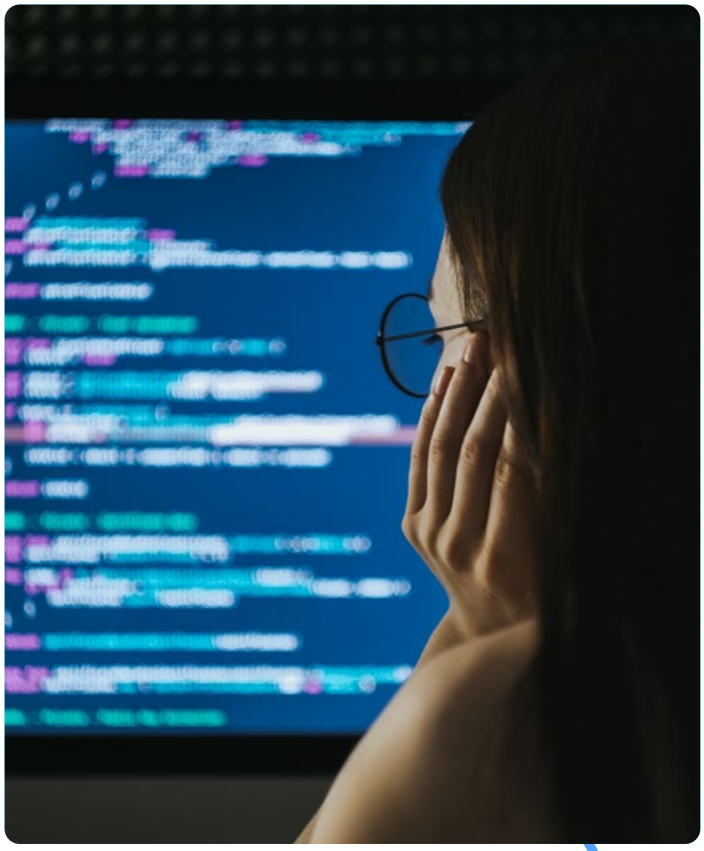
The pseudonymous ID is included in every telemetry event that is sent to Countly to represent a user instance.

The metrics include events such as a user opening the app, contributing (e.g., initiating a call), or encountering a decryption error.

If any of the above events are triggered, the following properties are sent along with the event type:
- Analytics identifier
- App version
- Device information (model, OS version)
- and whether the user is a team member

Team Admin Panel:
Team admins have access to the Web admin panel that is used to manage a Wire team. When the team admin decides to opt-in user metric collection for the admin panel, additional usage information of the admin panel is collected through Countly.

Crash reports

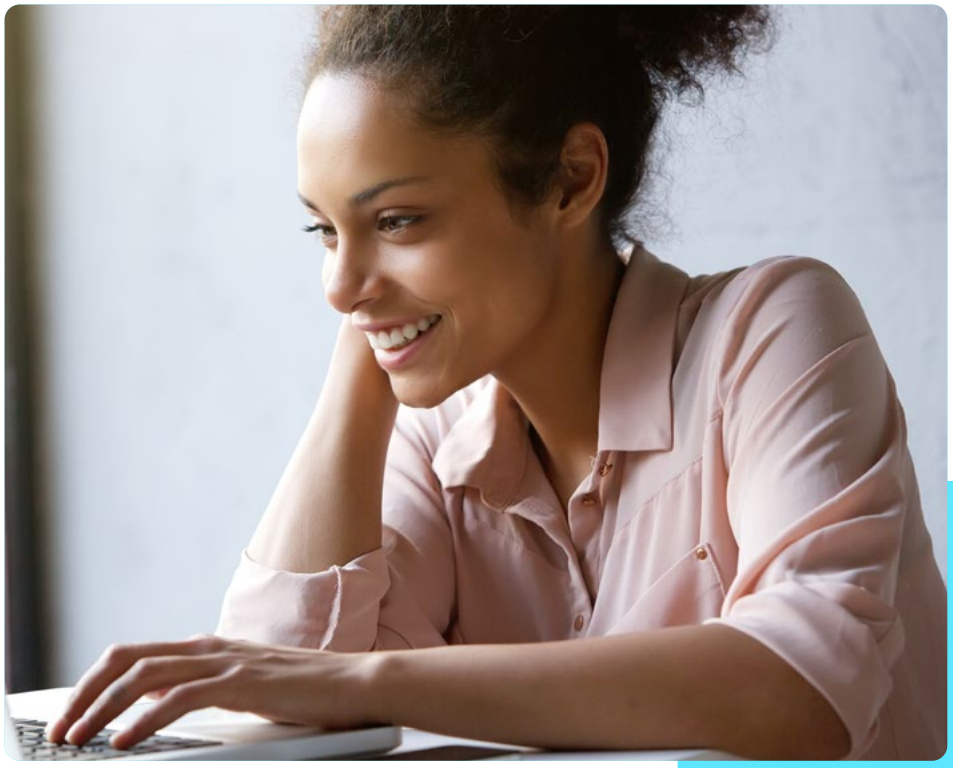


Crash reports
Crash reports are version-specific snapshots of an application's state captured when an execution failure occurs, typically when the operating system terminates the application unexpectedly. These reports are collected at the OS level, with no control from the app's code. Users can choose to send crash reports through an opt-in system, with the option to opt-out at any time. The opt-in/out, collection, and data transmission are managed by the operating system. The Wire MacOS and iOS apps use the Apple App Store for crash report collection, while the Wire Android app relies on the Google Play Store. These reports enable Wire to identify issues and implement bug fixes more efficiently.

Logs
Server-side logs are only kept for a maximum of 90 days, for the sole purpose of facilitating troubleshooting, improving the service and preventing abuse. Client-side logs are kept locally on clients and users can decide to manually share them.

Push notifications
Wire's mobile applications use FCM (Android) and APNS (Apple) as push notification providers. Users that do not want to rely on third-party push notification services, can use the F-Droid version of the app. It is preconfigured to bypass FCM, instead using only web sockets for notifications. While this approach may lead to increased battery consumption, it provides an alternative for users concerned about third-party involvement. Push notifications themselves do only contain the associated user identifier (UUID). They serve as a wake-up call, prompting the client to fetch all available messages for the provided user identifier from the Wire server message queue.

Wire for Enterprise

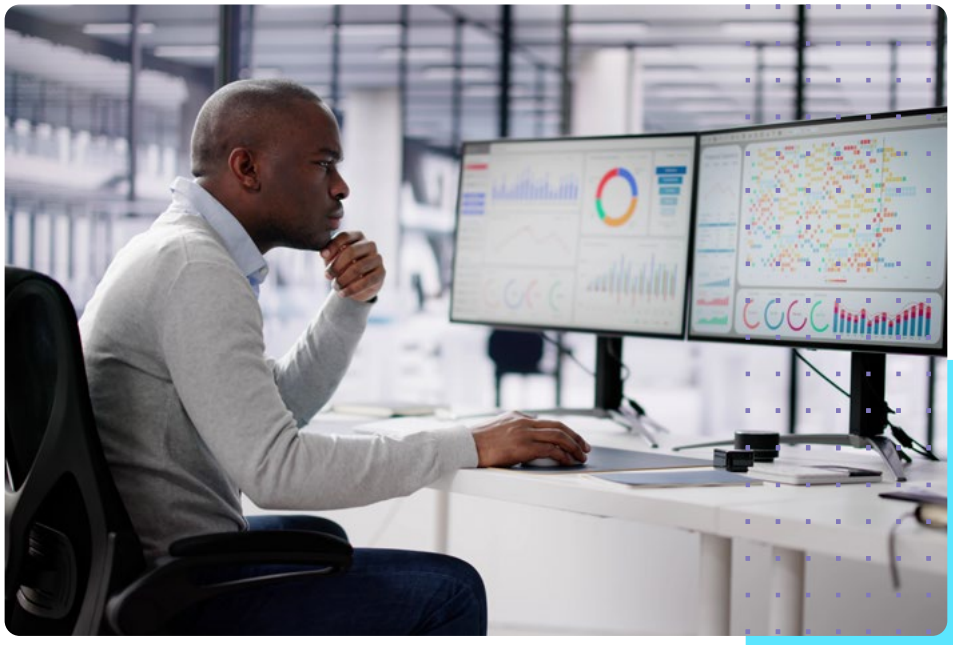


Wire for Enterprise uses the same technology and data as personal accounts, with the addition of the team membership for team accounts. Every team has at least one member, team admin, and team owner. Team owners can specify a billing address for invoicing purposes.

Billing

To make purchases through Wire services using a Team Admin account, Team Admins must provide a payment method and may be required to provide additional information such as billing address, phone number, email address, and zip code if required for tax purposes or to complete billing. In addition, other types of information related to the specific transaction may be collected, such as transaction amount and duration.

Payment information (such as credit card data) is exclusively handled by the billing providers (Stripe - https://stripe.com) and is not available to Wire. Furthermore, billing providers handle subscription information to determine invoice amounts. No personally identifiable user data from Wire is shared with billing providers. The only information shared alongside the billing information is the team administrator's email address.



Data deletion

Personal users can delete their accounts on their own, which triggers the removal of all information associated with that account. This can be done by navigating to the account section and selecting “Delete account”. In case of team accounts, the team administrator can delete the account which triggers the deletion of all account-related information.

Wire for Enterprise:
For paying customers, additional information is deleted from the customer relationship management system on demand.

Data export

Every user has the right to request an export of their data in accordance with GDPR regulations.

Contact Wire Support to get information about the data held or to get a copy of your data. The requested information will be available within the legally required timeframe. For more information, see our Privacy Policy.

Data security

Wire has implemented robust data security and protection measures to safeguard user privacy, in line with industry best practices. Our commitment includes a variety of technical and organizational measures (TOMs) designed to protect personal information from unauthorized access, loss, or misuse. These measures include encryption protocols, access controls, and regular security audits, ensuring that user data is handled securely.