Terms of service

Effective starting 26 November 2021

Ambire Wallet is an open-source non-custodial cryptocurrency wallet:

- open-source: the software is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and noninfringement
- non-custodial: it is designed such that each user account is solely controlled by whoever holds the associated private keys. In other words, the end user retains full custody (possession) of their crypto funds at all times. As such, loss of funds is possible if the end user loses control over their private keys, for example but not limited to: losing their passphrase, losing access to their JSON backup, etc. The end user is solely responsible for the control over their private keys.

Those characteristics, combined with the decentralized nature of blockchain technologies such as Ethereum, mean that no single party is able to freeze, repossess or in any other way control the funds and actions of end users.

By using Ambire Wallet, you agree not to hold it's contributors and authors financially accountable for any loss of funds resulting from user error, software error, unauthorized access (hacks), or otherwise.

Ambire Wallet contributors, authors and operators do not offer any business or investment advice. The content of the Ambire Wallet is not intended to be used as a guide for crypto-asset investments or signing of other legal agreements in connection to crypto-assets.

Ambire Wallet contributors, authors and operators shall not be held accountable for any actions performed by end users.

As open-source software, the Ambire Wallet source code can be copied locally and/or ran by any party, and as such it does not depend on any operators or service providers.

Any party may copy and develop the source code resulting in the formation of a distinct and separate software. The creation of forks cannot be avoided and end users are solely responsible for any losses and/or damages resulting from the use of forks.

The end users are solely responsible and liable for any and all of your actions and inactions on the application and all gains and losses sustained from their use of the Ambire Wallet. The end user hereby indemnifies Ambire Wallet contributors, authors

and operators in full for any and all negative consequences that might arise from the use of the application due to the lack of control over the peer-to-peer activities.

Due to the permissionless and decentralized nature, the access to the Ambire Wallet is granted worldwide. The use of the Wallet, however, may be legally prohibited or technically restricted in certain territories and countries. End users are solely responsible to inform themselves of such legal restrictions and to comply with the legal norms applicable for them. Technically speaking, due to the open-source nature of Ambire Wallet, access to your funds will always be possible as long as you retain access to any of the private keys controlling the account.

The activities conducted by the end users on the Wallet may result in the creation of a taxable event and end users may be objects of tax and fee payments to public authorities in different countries depending on the legal regulations. End users are obliged to inform themselves about such requirements and are solely responsible for their payments.

Software components

Ambire Wallet is composed of multiple software components, all of which can be used independently:

- smart contracts for EVM-based blockchains such as Ethereum, Polygon, Arbitrum, etc.
- user interface: front-end for desktop in the form of a single-page web application

While some components have undergone audits, this should not be treated as a warranty of any kind.

Login with email

When using the "login with email" feature, Ambire Wallet depends on an extra backend component. This component does not have access to or control over funds, but it may hold encrypted private key backups in case "Backup to Ambire Cloud" is enabled. This backend is not vital to the operation of the wallet: the account can be accessed without it as well.

Second key

When using the "login with email" feature, Ambire Wallet requires a secondary signature from a key that's held by said backend component. This key can be deleted from the backend component at user request, and/or exported by the user.

This key does not grant immediate access to user funds: it is used as an extra security measure (enabling email confirmation, 2FA) and to trigger account recovery, which is a timelocked request to change the account signer key that the user may cancel.

Opt-out

Any accounts created with "login with email" can be updated to function independently of this backend by simply adding another signer key in the form of Trezor, Ledger, Metamask or other, or by simply backing up the two (primary and secondary) keys.

Privacy Policy

Ambire Wallet stores no identifiable personal data, except an email address, only in the case of using the feature "Login with email & password". Should the user log-in with any of the other options (Metamask, Trezor, Ledger, etc.), no personal data is collected whatsoever. The addresses can be treated as indirect identifiers. An indirect identifier is a value which cannot be used alone to identify a data subject, however, could be identifying if combined with other indirect identifiers. Ambire Wallet does not in any way approve or control the appearance of this information on the application and this information can be permanently reflected on the blockchain which means that full deletion is not possible.

In the event that the email is collected, it is safely stored in a GDPR-compliant database, and not revealed to any third parties under any circumstances. The backend is SOC 2, CCPA and GDPR compliant.

Ambire Wallet is non-custodial and decentralized in nature, and as such it depends a backend only for "added value" features. This means that even non-personal data is only optionally stored on a backend.

As a non-custodial and privacy-focused solution, Ambire Wallet will not perform KYC or similar identity checks on it's users for it's core features.

Cookies

Ambire Wallet does not require or store any cookies, with the exception of Cloudflare cookies on the hosted version, which are non-identifiable and are required for the functioning of Cloudflare.