C Link Privacy Policy

Published on October 15, 2024.

Introduction

UAB Cambix located at Vilnius, Zalgirio g. 88-101, LT-09303, Lithuania, with registration number 306726345 ("we", "us", "our") is committed to protecting your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use the C Link Wallet and its associated website ("Platform").

Information We Collect

We collect personal information from our users in various ways, including when they register for an account, transfer tokens, or use our services. The types of personal information we collect may include:

- Name, email address, physical address, and phone number
- IP address, device type, and browser type
- Payment and transaction information, such as third-party wallet address information and C Link token holdings
- User-generated content, such as NFT metadata or transaction data
- Other details necessary to provide and improve our services
- Other information necessary to identify, assess, and manage risks related to money laundering and terrorist financing.

Information we collect automatically: We may collect certain information automatically when you use our services, such as your IP address, device type, browser type, and operating system.

Information we receive from third parties: We may receive information about you from third-party sources, such as social media platforms or payment processors. We may also receive information from our business partners, affiliates, or service providers.

We do not collect sensitive information unless the information is reasonably necessary for our business functions or activities. We will obtain your consent before collecting any sensitive information.

Our services are not intended for persons under the age of 18, and we do not knowingly or intentionally collect any personal information from, or market to, individuals under the age of 18. If you learn that an individual under the age of 18 has provided us with personal information contrary to these rules, please contact us as described in “Contact Us “section and we will delete the information from our systems.

How We Use Your Information

We use the personal information we collect to provide and improve our services, process payments and Web3 transactions, such as token transfers and staking, communicate with users, and analyze user behavior. Specifically, we use personal information to:

- Provide and improve our services, including to personalize the user experience, monitoring and analyze usage, and diagnosing technical issues,
- Process payments, including to verify identity and prevent fraudulent transactions,
- Communicate with users, including responding to inquiries and providing customer support, sending transactional messages, and sending promotional communications,
- Analyze user behavior, including to conduct market research, personalize content and advertising, and
- Comply with legal obligations, including such as to respond to legal requests and monitoring suspicious activity.

Legal Basis for Using Your Information

We process your personal information in accordance with the legal basis provided by applicable data protection laws, including the General Data Protection Regulation (GDPR). The primary legal basis for processing your personal information is to fulfill our contractual obligations to you when you use our services. This includes providing and improving our services, processing blockchain transactions, and communicating with you. Without processing your personal information, we would not be able to provide you with the services you have requested.

In certain cases, we may also process your personal information based on our legitimate interests. This may include analyzing user behavior to improve our services, conducting market research, and personalizing content and advertising. When we process your personal information based on our legitimate interests, we ensure that your rights and freedoms are not overridden by our interests. We conduct a balancing test to ensure that our legitimate interests are not outweighed by any potential impact on your privacy rights.

In addition, we may process your personal information to comply with legal obligations, such as responding to legal requests or preventing fraud and upholding AML and KYC compliance. In such cases, processing your personal information is necessary for compliance with a legal obligation that we are subject to.

If you have any questions about the legal basis for how we process your personal information, please contact us using the information provided in the "Contact Us" section below.

In certain situations, we may rely on your consent as the legal basis for processing your personal information. If you have provided consent for the processing of your personal information, you have the right to withdraw that consent at any time. To do so, please contact us using the details provided in the "Contact Us" section below.

How We Share Your Information

We may share personal information with third parties, such as payment processors, advertising partners, and third-party service providers, to provide and improve our services. Specifically, we may share personal information to:

- For legal purposes: We may share your information with third parties if we are required to do so by law, such as in response to a court order or a legal request from a government agency.
- In case of a merger or acquisition: We may share your information in the event of a merger, acquisition, or other business transaction.
- With your consent: We may share your information with third parties if you have given us your consent to do so.

We require the third-party service providers acting on our behalf or with whom we share your information to provide appropriate security measures in accordance with industry standards and in compliance with this Policy, their privacy and security obligations, and any other appropriate confidentiality and security measures.

International Data Transfers

We may transfer personal data to countries outside of the European Union (EU) and the European Economic Area (EEA). When doing so, we will take appropriate measures to ensure that the data is protected and that the transfer complies with applicable data protection laws.

The transfer of personal data outside of the EU/EEA may take place in the following situations:

- We may transfer personal data to our third-party service providers or partners located outside of the EU/EEA in order to provide the services you have requested or to perform other functions on our behalf, such as hosting Digital Wallet services, our website, or processing transactions. These transfers are subject to appropriate safeguards, such as standard contractual clauses or certification, to ensure that the data is adequately protected. In some cases, we have adopted measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
- If you are located outside of the EU/EEA and use our services, your personal data may be transferred to our servers in the EU/EEA or to third-party service providers or partners located outside of the EU/EEA. In such cases, we will ensure that appropriate safeguards are in place to ensure that the transfer is legal and that the data is adequately protected.

Cookies and Similar Technologies

We use cookies and similar technologies to enhance your user experience and to analyze how our website is used. Cookies are small text files that are placed on your device when you visit our website. They are used to remember your preferences, facilitate navigation, and improve our website. Refer to our Cookie Use Policy for additional information about cookies used on our website.

How We Protect Your Information

We use a variety of industry-standard security measures to protect your personal information from unauthorized access, use, disclosure, alteration, and destruction. Specifically, we use Fireblocks, which provides a suite of applications to manage digital asset operations. Fireblocks employ Multi-Layer Security that eliminates a single point of compromise with Multi-Party Computation (MPC) and leverages secure hardware enclaves to ensure key material is isolated, protected, and resistant to unauthorized access. Additionally, the Fireblocks Policy Engine provides a critical layer of governance to protect against insider threats and attackers.

Examples of common security measures include:

- Encryption: We may encrypt your personal information when it is transmitted over the internet to help protect against unauthorized access.
- Access controls: We may limit access to your personal information to authorized personnel who have a legitimate need to access the information.
- Firewalls: We may use firewalls to help prevent unauthorized access to our systems and networks.
- Intrusion detection/prevention systems: We may use intrusion detection/prevention systems to detect and prevent unauthorized access or attacks on our systems and networks.
- Physical security: We may use physical security measures, such as secure facilities and access controls, to protect against unauthorized access to our premises and equipment.

You can play a role in keeping your personal data secure by maintaining the confidentiality of any passwords and accounts used in relation to our services, websites, or materials. We recommend that you use a unique password that you do not use on any third-party websites or related services. Please do not disclose any passwords used in connection with our services, websites, or materials to third parties.

If you become aware of any unauthorized access to your account or other security breach, please notify us immediately so that we can take appropriate action to investigate and mitigate the incident.

Data Retention and Deletion

We will retain your personal information for as long as necessary to fulfill the purposes for which it was collected, including for the purposes of satisfying any legal, accounting, or

reporting requirements. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements.

In general, we will retain your personal information for the duration of your account with us, and for a reasonable period of time afterwards, in order to maintain business records for analysis and/or audit purposes, to comply with legal or regulatory requirements, and for other legitimate storage purposes.

If the storage purpose is no longer given or a prescribed retention period expires, we will delete your personal data.

Client Rights and Complaint Handling

You have certain rights in relation to your personal information. Subject to certain limitations on certain rights, you have the following rights in relation to your personal information:

- Right to access: You have the right to request copies of your personal information.
- Right to rectification: You have the right to request that we correct any information you believe is inaccurate. You also have the right to request that we complete the information you believe is incomplete.
- Right to erasure: You have the right to request that we erase your personal information, under certain conditions.
- Right to restrict processing: You have the right to request that we restrict the processing of your personal information, under certain conditions.
- Right to object to processing: You have the right to object to our processing of your personal information, under certain conditions.
- Right to data portability: You have the right to request that we transfer the data that we have collected to another organization, or directly to you, under certain conditions.
- Right to withdraw consent: You have the right to withdraw your consent at any time when we rely on your consent to process your personal information.

If you wish to exercise any of these rights, please contact us using the details provided in the "Contact Us" section below. We may need to verify your identity before processing your request. We will try to respond to your request within a reasonable timeframe.

The specified requests are free of charge, except when the requests are clearly unreasonable, repetitive or excessive, in which case we may charge a reasonable fee based on administrative cost of providing the information or taking the action requested. If the user requests additional copies of their personal data after the initial copy has been provided, a reasonable fee may be charged.

Please note that we may need to retain certain information for recordkeeping purposes and/or to complete any transactions that you began prior to requesting a change or deletion. There may also be residual information that will remain within our databases and other records, which will not be removed.

We encourage you to keep your personal information up-to-date. You have a responsibility to inform us of any changes to your personal information to ensure that it remains accurate and up-to-date. If you suspect that your personal information has been misused or if you become aware of any unauthorized use or access of your personal information, please contact us immediately at contact@cambix.com so that we can take appropriate action to investigate and address the situation.

Compliance with Markets in Crypto-Assets Regulation (MICA)

As a Crypto-Asset Service Provider (CASP) under the Markets in Crypto-Assets Regulation (MiCA), we are subject to additional obligations concerning personal data and transparency. Accordingly, we shall implement the following measures:

- **Record-Keeping Obligations.** We maintain records of all crypto-asset services, activities, orders, and transactions for a period as required by applicable laws and regulations. These records are kept to ensure compliance with our legal obligations and to provide transparency to our clients.

- **Disclosure of Conflicts of Interest.** We implement and maintain policies and procedures to identify, prevent, manage, and disclose conflicts of interest. Information about the general nature and sources of conflicts of interest and the steps taken to mitigate them will be available on our website.

- **Public Disclosure of Inside Information.** We will publicly disclose inside information in a manner that ensures fast access and complete, correct, and timely assessment by the public. This information will be posted and maintained on our website for a period of at least five years.

- **Client Awareness of Risks.** We ensure that our clients are aware of the risks involved in purchasing crypto-assets. Detailed information about these risks is provided in the Terms of Service.

Changes to This Policy

We may update this privacy policy from time to time to reflect changes in our services, applicable laws, or best practices. We will notify you of any material changes to the policy and provide the updated policy on our website.

Contact Us

If you have any questions or concerns about this Privacy Policy, please contact us using the details provided on our website or by emailing contat@cambix.com.

This updated Privacy Policy is designed to ensure compliance with MiCA and provide a clear and concise overview of how Cambix handles personal data for users of C Link and its associated website and services.

Supervisory data proception authority

Data subjects have the right to lodge a complaint with a supervisory authority if they believe that their rights have been infringed. In Lithuania, the supervisory authority is the State Data Protection Inspectorate. Data subjects also have the right to lodge a complaint with a supervisory authority in the EU Member State where they reside, work or where the alleged infringement took place. If the supervisory authority in another EU Member State is contacted, the complaint will be forwarded to the appropriate supervisory authority.

If you believe that we have not complied with this Privacy Policy or applicable data protection laws, you have the right to lodge a complaint with the Data Protection Authority at the following:

Phone: +370 5 271 2804 / 279 144
E-mail: ada@ada.lt
Postal address: L. Sapiegos str. 17, LT-10312 Vilnius