



Nature's Ledger

Nature's Ledger Privacy and Data Management Policy

Revised: May 4, 2026

This Privacy and Data Management Policy applies to all users of Nature's Ledger's cryptocurrency exchange platform (the "NLX"), websites, mobile applications, and related services provided by its majority-owned subsidiaries with specific provisions for residents of the United States and Canada.

1. INTRODUCTION

Nature's Ledger and its majority-owned subsidiaries ("**Company**", "**We**", "**Us**", or "**Our**") respect your privacy and are committed to protecting it in accordance with this Privacy and Data Management Policy ("**Policy**" or "**Privacy Policy**"). We understand how important your privacy is, and we are dedicated to safeguarding your personal information in compliance with applicable privacy laws, including the Personal Information Protection and Electronic Documents Act (**PIPEDA**) and applicable provincial privacy legislation in Canada, the California Consumer Privacy Act as amended by the California Privacy Rights Act (**CCPA/CPRA**), and other applicable United States federal and state privacy laws.

This Policy describes:

- How we collect, use, disclose, and protect the personal information of our customers, platform users, and website visitors ("you" or "your").
- The types of information we may collect from you or that you may provide when you use our cryptocurrency exchange platform, visit our website at www.Naturesledger.com or our subsidiary domains (our "Website"), or use our mobile applications and related services (collectively, the "Services").
- Our practices for collecting, using, maintaining, protecting, and disclosing that information.
- Your rights regarding your personal information under applicable law.

We will only use your personal information in accordance with this Policy unless otherwise required by applicable law. We take steps to ensure that the personal information that we collect about you is adequate, relevant, not excessive, and used for limited purposes.

Privacy laws in Canada generally define "**personal information**" as any information about an identifiable individual, which includes information that can be used on its own or with other information to identify, contact, or locate a single person. Under the CCPA/CPRA, "**personal information**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

1.1 Scope of This Policy

This Policy applies to information we collect, use, or disclose about you:

- On our Website or through our cryptocurrency exchange platform.
- Through our mobile and desktop applications.
- In email, text, and other electronic messages between you and the Company.
- When you interact with our advertising and applications on third-party websites and services, if those applications or advertising include links to this Policy.
- Through our customer support, identity verification, and Know Your Customer ("KYC") processes.
- Through any marketing or communications initiatives related to our corporate offerings.
- When facilitating connections between users and our representatives, partners, or affiliates.

The Website and Services may include links to third-party websites, plug-ins, services, social networks, or applications. Clicking on those links or enabling those connections may allow the third party to collect or share data about you. We do not control these third-party websites, and we encourage you to read the privacy policy of every website you visit.

Important: By accessing or using our Services, you indicate that you understand, accept, and consent to the practices described in this Policy. If you do not agree with our policies and practices, your choice is not to use our Services.

2. INFORMATION WE COLLECT ABOUT YOU

We collect and use several types of information from and about you to comply with legal and regulatory requirements and provide you with our Services. The categories of information we collect include:

2.1 Personal and Identity Information

Information that we can reasonably use to directly or indirectly identify you, including:

- Full legal name, date of birth, and gender.
- Mailing address, email address, and telephone number.
- Social Security Number (SSN), Social Insurance Number (SIN), or other government-issued identification numbers, only where required by law for identity verification, tax reporting, or regulatory compliance.
- Government-issued photo identification (e.g., passport, driver's licence, national identity card).
- Photographs, selfies, or video recordings submitted for identity verification purposes.
- **Biometric information**, including facial recognition data, voiceprints, and other biometric identifiers collected during identity verification and KYC processes, to the extent permitted by applicable law.

2.2 Financial and Transactional Information

- Bank account details, credit or debit card numbers, and other payment instrument information.
- Cryptocurrency wallet addresses and blockchain transaction data.
- Transaction history, including details of purchases, sales, trades, transfers, deposits, and withdrawals of cryptocurrency and fiat currency.
- Source of funds and wealth information, where required for regulatory compliance.
- Tax identification information as required under applicable law.

2.3 Technical and Device Information

- Internet Protocol (IP) address, device identifiers, browser type and version, time zone setting, and operating system.
- Browser plug-in types and versions, device type, and platform.
- Login information, access timestamps, and session data.
- Information about your internet connection and the equipment you use to access our Services.

2.4 Usage and Behavioural Information

- Full Uniform Resource Locators (URLs), clickstream data to, through, and from our Website.
- Products, services, or features you viewed, searched for, or interacted with.
- Page response times, download errors, length of visits to certain pages, and page interaction information (such as scrolling, clicks, and mouse-overs).
- Methods used to browse away from the page.
- Aggregate and statistical data derived from your usage patterns.

2.5 Communications and Correspondence

- Records and copies of your correspondence with us, including emails, chat transcripts, and support tickets.
- Responses to surveys, research, or promotional activities.
- Feedback, reviews, or comments you submit.

2.6 Information from Third-Party Sources

- Information from identity verification and KYC/AML service providers.
- Publicly available information, including from blockchain networks and public registries.
- Information from credit reporting agencies and fraud prevention services.
- Information from business partners, affiliates, and referral sources.
- Information from government agencies and regulatory bodies, as permitted by law.

3. HOW WE COLLECT INFORMATION ABOUT YOU

We use different methods to collect your information, including through:

3.1 Direct Interactions

You provide information directly to us when you:

- Create an account or register for our Services.
- Complete our identity verification and KYC processes.
- Execute trades, deposits, withdrawals, or other transactions on our platforms.
- Subscribe to communications, newsletters, or marketing materials.
- Contact our customer support team.
- Participate in surveys, promotions, or contests.
- Fill in forms on our Website or through our applications.

3.2 Automated Technologies and Interactions

As you navigate through and interact with our Website and Services, we may use cookies or other automatic data collection technologies to collect certain information about your equipment, browsing actions, and patterns, including:

- **Cookies (browser cookies):** Small files placed on the hard drive of your device. You may refuse to accept browser cookies by activating the appropriate setting on your browser. However, if you do so, you may be unable to access certain parts of our Services.
- **Web beacons:** Small electronic files (also referred to as clear gifs, pixel tags, and single-pixel gifs) contained in pages of our Website and emails that permit us, for example, to count users who have visited those pages or opened an email, and for other related website statistics.
- **Analytics tools:** We may use third-party analytics services (such as Google Analytics) to collect and analyse usage information.
- **Blockchain data:** We may monitor public blockchain networks to verify transaction information and wallet addresses associated with your account.

3.3 Third-Party Sources

We may receive information about you from third parties, including:

- Identity verification and fraud detection service providers.
- Financial institutions and payment processors.
- Public blockchain networks and data aggregation services.
- Government agencies, regulatory authorities, and law enforcement, to the extent permitted by applicable law.
- Our business partners, affiliates, and referral networks.

4. HOW WE USE YOUR INFORMATION

We use information that we collect about you or that you provide to us, including any personal information:

4.1 To Provide and Operate Our Services

- To create, manage, and maintain your account.
- To process transactions, including the purchase, sale, and exchange of cryptocurrencies.
- To verify your identity and conduct KYC and anti-money laundering (AML) checks as required by applicable law, including requirements under the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and the Financial Crimes Enforcement Network (FinCEN).
- To present our Website and Services and their contents to you.
- To provide customer support and respond to your inquiries.

4.2 For Compliance and Legal Purposes

- To comply with applicable laws, regulations, and legal processes, including AML and counter-terrorist financing (CTF) obligations.
- To submit regulatory reports, including suspicious transaction reports (STRs), suspicious activity reports (SARs), large cash transaction reports (LCTRs), large virtual currency transaction reports (LVCTRs), and currency transaction reports (CTRs) as required by FINTRAC, FinCEN, and other applicable regulators.
- To comply with the Travel Rule as mandated by FINTRAC (for transactions exceeding CAD \$1,000) and FinCEN (for transactions exceeding USD \$3,000), which requires the collection and transmission of sender and recipient identifying information, including names, account numbers, and addresses, to the receiving virtual asset service provider.
- To comply with beneficial ownership requirements and sanctions screening under the Office of Foreign Assets Control (OFAC) and applicable Canadian sanctions regimes.
- To enforce our terms of use, user agreements, and other contractual obligations.
- To respond to court orders, subpoenas, search warrants, government or regulatory requests, and other lawful demands.

4.3 For Security and Fraud Prevention

- To detect, investigate, and prevent fraudulent transactions, unauthorized access, and other illegal activities.
- To protect the rights, property, or safety of the Company, our customers, or others.
- To monitor and analyse platform activity for potential security threats.

4.4 For Marketing and Communications

- To inform you about our products, services, programs, events, and news updates, including **specific cryptocurrency offerings and token listings** that may be of interest to you.
- To send you promotional communications about our own and, where you have consented, third-party cryptocurrency products and services.
- To personalise and tailor marketing content and advertisements based on your interests, transaction history, and usage patterns.
- To measure or understand the effectiveness of advertising we serve to you and others, and to deliver relevant advertising.

Opt-Out: If you do not want us to use your information for marketing purposes, you may opt out at any time by using the unsubscribe mechanism at the bottom of our emails, adjusting your communication preferences in your account settings, or emailing us at info@naturesledger.com. Please note that you may still receive transactional or account-related communications from us.

4.5 For Improvement and Analytics

- To improve our Website, platform, products, services, marketing, and customer experience.
- To conduct research and analysis on usage patterns and market trends.
- To estimate our audience size and usage patterns.

4.6 Artificial Intelligence and Automated Decision-Making

We utilise artificial intelligence (“AI”) systems, processes, and AI agents to facilitate the effective use of information collected, propose offers unique to certain users, assess risk profiles, enhance fraud detection, and may incorporate the information obtained in system workflows. By agreeing to the use of our Services or participating in any platform, system, network, or exchange operated by us, you expressly consent to the use of your information and the potential for its use and availability through AI systems and agents, to the extent permitted by applicable law.

Where automated decision-making has a significant impact on you, you may have the right under applicable law to request human review of such decisions.

5. HOW WE SHARE YOUR INFORMATION

5.1 Affiliates and Service Providers

We may transfer your personal information to our affiliates and the following categories of third-party service providers, who are contractually obligated to keep personal information confidential and use it only for the purposes for which we disclose it to them:

- Identity verification and KYC/AML compliance providers (e.g., document verification, biometric authentication, and sanctions screening services).
- Financial institutions, payment processors, and banking partners.
- Cloud hosting, data storage, and IT infrastructure providers.
- Fraud detection and cybersecurity service providers.
- Data analytics and business intelligence providers.
- Marketing, advertising, and communications platforms.
- Customer support and communication tools providers.
- Legal, accounting, and professional advisory service providers.

- Blockchain analytics and transaction monitoring providers.

5.2 Regulatory and Legal Disclosures

In certain cases, we and our Canadian, U.S., or other foreign service providers may disclose your personal information:

- In response to a valid search warrant, subpoena, inquiry, court order, or other lawful request.
- To comply with applicable laws, regulations, or regulatory requirements, including reports required by FINTRAC, FinCEN, or other applicable regulators.
- To other organisations for the purposes of investigating breaches of agreements, contraventions of laws, fraud detection, suppression, prevention, or as required or permitted by applicable Canadian, U.S., or other laws.
- Where legally permitted, we will endeavour to provide you with prompt notice of such legal requirements so that you may seek an appropriate protective order or other remedy at your own cost and expense.

5.3 Business Transfers

In the event of a corporate merger, consolidation, sale of assets, share sale, investment transaction, or other corporate rearrangement or business venture, we may sell, transfer, or disclose our database of personal information to an actual or potential successor entity, purchaser, or investor. We will endeavour to ensure such party is bound by appropriate obligations to use or disclose personal information in a manner consistent with this Policy.

5.4 Blockchain Disclosures

Important: Certain cryptocurrency transactions are recorded on public blockchain networks. When you engage in a transaction on a public blockchain, certain transaction data (such as wallet addresses, transaction amounts, and timestamps) becomes publicly available and cannot be deleted or modified by us. We do not control public blockchain networks and are not responsible for the public availability of information recorded thereon.

5.5 Aggregated and De-Identified Data

We may disclose aggregated or de-identified information about our users, which does not identify any individual, without restriction and for any legitimate business purpose.

6. INTERNATIONAL DATA TRANSFERS

We may process, store, and transfer your personal information in and to foreign countries, including the United States and Canada, with privacy laws that may or may not be as comprehensive as the laws in your jurisdiction. In these circumstances, the governments, courts, law enforcement, or regulatory agencies of that country may be able to obtain access to your personal information through the laws of the foreign country.

Whenever we engage a service provider located outside of your jurisdiction, we require that its privacy and security standards adhere to this Policy and applicable privacy legislation. Our service providers may be located in the United States, Canada, or other foreign jurisdictions. If you have any questions regarding transfers to foreign affiliates or third-party service providers, including their processing locations and purposes, please contact our Privacy Officer.

By submitting your personal information or engaging with the Services, you consent to this transfer, storage, or processing.

7. SECURITY AND RETENTION OF YOUR PERSONAL INFORMATION

7.1 Security Measures

We prioritise the security of your personal information and employ suitable physical, technical, and organisational measures to protect it against unauthorised or unlawful processing, accidental loss, destruction, or damage. These measures include:

- Encryption of data in transit and at rest, including the use of SSL/TLS technology for data transmission.
- Multi-factor authentication and secure access controls.
- Regular security assessments, vulnerability testing, and penetration testing.
- Employee training and awareness programs on data protection and privacy.
- Storage of information behind firewalls on secure servers.

We represent and warrant that we comply, and require our employees and service providers to comply, with all applicable federal, provincial, and state data protection and privacy laws and regulations in the maintenance, disclosure, and use of all personal information.

The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of our Services, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

Disclaimer: Unfortunately, the transmission of information via the Internet is not completely secure.

Although we do our best to protect your personal information, we cannot guarantee the security of your personal information transmitted to or through our Services. Any transmission of personal information is at your own risk.

7.2 Breach Notification

In the event of a data breach involving your personal information that creates a real risk of significant harm to you, we will notify you and the applicable regulatory authorities as required by law, including:

- The Office of the Privacy Commissioner of Canada, as required under PIPEDA's mandatory breach reporting requirements (for Canadian residents).
- Applicable U.S. state attorneys general and affected individuals, in accordance with state data breach notification laws (notification timelines vary by state; for example, 72 hours in some jurisdictions, 30–60 days in others).
- Other applicable regulators as required by law.

Such notification will include a description of the nature of the breach, the personal information affected, the steps we have taken or propose to take to address the breach, and contact information for further inquiries.

7.3 Data Retention

Except as otherwise permitted or required by applicable law or regulation, we will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Specific retention periods include:

- **KYC/AML records (identity documents, verification data, transaction records):** Minimum five (5) years following the closure of your account or the completion of a transaction, as required by FINTRAC and FinCEN regulations, or longer as required by applicable law.

- **Financial and tax records:** Seven (7) years or as required by applicable tax and accounting laws.
- **General account information:** Duration of your account relationship plus five (5) years, or as required by law.
- **Marketing and communications preferences:** Until you withdraw consent or close your account.
- **Technical and usage data (cookies, analytics):** Up to twenty-four (24) months from the date of collection, unless a longer period is required for security or fraud investigation purposes.
- **Customer support records:** Three (3) years following resolution of the inquiry, or as required by law.

Under some circumstances, we may anonymise your personal information so that it can no longer be associated with you. We reserve the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to you or your consent.

8. YOUR RIGHTS REGARDING YOUR PERSONAL INFORMATION

8.1 Access and Correction

You have the right to request access to the personal information we hold about you and to request correction of any inaccurate or incomplete personal information. You may exercise these rights by:

- Logging into your account and reviewing your account profile.
- Contacting our Privacy Officer in writing or by emailing your request to info@naturesledger.com.

We may request specific information from you to help us confirm your identity and your right to access. We will respond to your request in a timely manner; however, we may require satisfactory verification of your identity before disclosing any personal information. Applicable law may allow or require us to refuse to provide you with access to some or all of the personal information that we hold about you, and we will inform you of the reasons for any refusal, subject to any legal or regulatory restrictions.

8.2 Withdrawal of Consent

Where you have provided your consent to the collection, use, and transfer of your personal information, you may have the legal right to withdraw your consent under certain circumstances. To withdraw your consent, if applicable, contact us at info@naturesledger.com. Please note that:

- Withdrawal of consent may result in the inability to provide certain Services to you, as we may be legally required to retain certain information for regulatory compliance.
- We cannot delete personal information that we are required by law to maintain (e.g., KYC records, transaction records required by FINTRAC or FinCEN).
- We will explain the impact of withdrawal to you to help you with your decision.

8.3 Rights of Canadian Residents

If you are a resident of Canada, you have the following rights under PIPEDA and applicable provincial privacy legislation:

- The right to access your personal information held by us.
- The right to challenge the accuracy and completeness of your personal information and have it amended as appropriate.
- The right to withdraw consent to the collection, use, or disclosure of your personal information, subject to legal or contractual restrictions and reasonable notice.

- The right to file a complaint with the Office of the Privacy Commissioner of Canada if you believe your privacy rights have been violated.

8.4 Rights of United States Residents

If you are a resident of the United States, you may have additional rights depending on your state of residence:

California Residents (CCPA/CPRA)

If you are a California resident, you have the right to:

- **Know and Access:** Request that we disclose the categories and specific pieces of personal information we have collected about you, the categories of sources from which the information was collected, the business or commercial purpose for collecting the information, and the categories of third parties with whom we share personal information.
- **Delete:** Request that we delete personal information we have collected from you, subject to certain exceptions.
- **Correct:** Request that we correct inaccurate personal information that we maintain about you.
- **Opt-Out of Sale or Sharing:** Direct us not to sell or share your personal information for cross-context behavioural advertising purposes. We do not sell personal information in the traditional sense; however, certain activities such as targeted advertising may constitute “selling” or “sharing” under the CCPA/CPRA.
- **Non-Discrimination:** Not be discriminated against for exercising your privacy rights.
- **Limit Use of Sensitive Personal Information:** Request that we limit the use or disclosure of your sensitive personal information to purposes necessary to perform our Services.

Other U.S. State Privacy Laws

Residents of Virginia, Colorado, Connecticut, Utah, and other states with comprehensive privacy legislation may have similar rights, including rights to access, correct, delete, and opt out of certain processing activities. Please contact our Privacy Officer to inquire about your specific rights.

8.5 Managing Cookies and Tracking

You have the option to limit the collection of certain website information by deleting or disabling cookies. Most internet browsers allow you to erase stored cookies, block all cookies, or receive a warning before a cookie is stored. Disabling cookies may impact your ability to use specific features of our Services. You can also opt out of interest-based advertising through:

- The [Digital Advertising Alliance of Canada](#)
- The [Network Advertising Initiative](#)
- The [Digital Advertising Alliance \(U.S.\)](#)

Please be aware that many opt-out mechanisms utilise browser cookies or device controls and are specific to the device or browser you are using. If you change devices, switch web browsers, or delete cookies, you may need to opt out again.

9. THIRD-PARTY USE OF COOKIES AND TRACKING TECHNOLOGIES

Some content or applications on the Website are served by third parties, including advertisers, ad networks and servers, content providers, and application providers. These third parties may use cookies, alone or in conjunction with web beacons or other tracking technologies, to collect

information about you when you use our Services. The information they collect may be associated with your personal information or they may collect information, including personal information, about your online activities over time and across different websites and other online services.

We do not control these third parties' tracking technologies or how they are used. If you have any questions about an advertisement or other targeted content, you should contact the responsible provider directly.

10. CHILDREN'S PRIVACY

Our Services are not intended for children under 18 years of age. No one under age 18 may provide any personal information to or through the Services. We do not knowingly collect personal information from children under 18. If you are under 18, do not use or provide any information on our Services, register on the platform, make any transactions, or provide any information about yourself to us.

If we learn we have collected or received personal information from a child under 18 without verification of parental consent, we will delete that information. If you believe we might have any information from or about a child under 18, please contact us at info@naturesledger.com.

11. DO NOT TRACK SIGNALS

Some web browsers transmit "Do Not Track" signals to the websites and other online services with which a user communicates. There is currently no universally accepted standard for how companies should respond to these signals. We currently do not respond to "Do Not Track" browser signals or similar mechanisms. We will review our practices if and when a formal standard is established and accepted.

12. CHANGES TO THIS PRIVACY POLICY

This Privacy Policy will be periodically reviewed to account for new laws, technologies, and changes in our operations. We recommend that you periodically review this Policy for any updates. We reserve the right to amend this Privacy Policy from time to time.

If we make material changes to how we treat our users' personal information, we will notify you by email to the primary email address associated with your account and through a notice on our Website. We include the date the Privacy Policy was last revised at the top of this document. You are responsible for ensuring we have an up-to-date, active, and deliverable email address for you.

13. CONSENT

We restrict the collection of personal information to what is necessary to meet the purpose intended. We require the consent of the individual prior to collecting, using, or disclosing their personal information. Your consent to the collection, use, and disclosure of information may be express, deemed, or implied from your conduct with us, your actions, or your inaction. We may ask for your consent in writing or electronically, but in some circumstances, we may accept your oral consent.

By accessing or receiving a copy of this Privacy Policy, creating an account, or providing personal information to us, unless you advise us otherwise, you will be deemed to have given consent to the collection, use, and disclosure of your personal information in accordance with and for the purposes stated in this Privacy Policy.

Please note: You have the right, as permitted by applicable law, to withdraw your consent for us to use or disclose your personal information at any time. If you wish to withdraw your consent, please contact our Privacy Officer. It is important to be aware that withdrawing consent may result in the inability to provide certain Services to you. Additionally, certain information may be required to be retained under AML/CTF laws regardless of withdrawal of consent.

14. GENERAL PROVISIONS

This Privacy Policy is not intended to create or confer upon any individual any rights or impose upon the Company any rights or obligations outside of, or in addition to, any rights or obligations imposed by applicable federal, provincial, and state privacy laws. If any term or provision of this Privacy Policy is invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability shall not affect any other term or provision of this Privacy Policy or invalidate or render unenforceable such term or provision in any other jurisdiction.

Should there be, in any specific case, any inconsistency between this Privacy Policy and applicable federal, provincial, or state privacy laws, this Privacy Policy shall be interpreted to give effect to and comply with such privacy laws.

15. CONTACT INFORMATION AND CHALLENGING COMPLIANCE

We welcome your questions, comments, and requests regarding this Privacy Policy and our privacy practices. Please contact us at:

[Privacy Officer]

Nature's Ledger Inc.

002-2305 Victoria Avenue, Regina, Saskatchewan, S4V 0S7, Canada

Email: info@naturesledger.com

Telephone Number: +1 (306) 352 6132

We have procedures in place to receive and respond to complaints or inquiries about our handling of personal information, our compliance with this Policy, and applicable privacy laws. To discuss our compliance with this Policy, please contact our Privacy Officer using the contact information listed above.

For Canadian residents: If you are not satisfied with our response to your complaint, you have the right to file a complaint with the Office of the Privacy Commissioner of Canada at www.priv.gc.ca, or with your applicable provincial privacy commissioner.

For California residents: You may also contact the California Attorney General's Office for information about your rights under the CCPA/CPRA.

For other U.S. residents: You may contact your state attorney general's office for information about your rights under applicable state privacy laws.