Privacy Notice

Last updated: 31.12.2025

Version: 2.1

This Privacy Notice (the "**Notice**") describes how we collect and process your data through https://kolo.xyz/ and/or https://kolo.in/ website, Telegram Mini App available at https://t.me/kolo and related mobile applications (Android / iOS) (together, the "**Site(s)**"). The terms "**we**", "**us**", "**our**" and "**ourselves**" refer to the KOLO entities, such as BURVIX SP. Z O. O., a legal person registered under the laws of Poland, and Hardline Holdings Limited, a legal person registered under the laws of the Republic of Kazakhstan.

We are committed to safeguarding the privacy of our users. We are not going to misuse your data.

Depending on the services offered to you, there will be one or both of the following data controllers processing your data. Please refer to our Terms of Use to find out which entity will act as your data controller or contact us using contact information below.

Controllers details:

BURVIX SP. Z O. O.

Registration number: 0001131882

Registered address: ul. Żurawia 43, lok. 8a, 00-680 Warszawa, Poland

Contact email address: support@kolo.xyz

Hardline Holdings Limited

Registration number: 221240900259

Registered address: Z05T3F6, Astana, Esil district, 55/18, Mangilik El, office 218, Kazakhstan

Contact email address: support@kolo.xyz

Data Protection Officer

We have appointed a Data Protection Officer (DPO) based in the United Kingdom for data protection matters, in accordance with Art. 37 of the GDPR. You can address Legal Nodes any questions about our processing of your personal data, including any requests to exercise your rights provided by the General Data Protection Regulation (EU) 2016/679. You can contact our DPO using the details set out below.

DPO's contact details:

Legal Nodes Ltd

Office 2, Bennet's House, 21 Leyton Road, Harpenden, England, AL5 2HU

E-mail: kolo.dpo@legalnodes.com

Consent for Data Processing and Transfers (Kazakhstan Users Only)

By using the services of Hardline Holdings Limited, the users from the Republic of

Kazakhstan hereby give their explicit consent to the processing of their personal data as outlined in this Notice, including any transfers of their personal data to other countries, in accordance with the terms and purposes described herein.

Table of contents:

What Personal Data We Collect

We collect various types of personal data to provide and improve our card wallet services. The data we collect includes, but is not limited to:

- **Login credentials** such as email address;
- **Personal details, contact details, and identifiers:** name, pronoun, identifiers (all types), contact details, email, phone numbers, physical address, gender, date of birth, age, place of birth, Google and Google OAuth authentication data;
- **Profile data:** user name, password, unique ID/public ID, Telegram ID, nickname, language, telephone number, profile picture, preferences (language, marketing preferences);
- **KYC data:** verification data, passports (ID document), email, phone number, questionnaire, liveness, selfie, biometric data, residence address, proof of address, Politically Exposed Person (PEP), sanctions, adverse media;
- **KYB data:** company details, registration, extracts, beneficial owner, directors;
- **Financial data and transaction data:** bank account, payment card details, wallet addresses, virtual currency accounts, stored value accounts, amounts associated with accounts, annual income range, source of funds and related documentation, details about payments to and from an individual, bank account and payment card details, wallet addresses, details about payments to or from the customers;
- **Questionnaire data:** financial details (e.g., expected monthly turnover, the source of funds) and employment status;
- **Risk score** generated on the basis of the verification check;
- **Commercial information:** history and records of products and services obtained, correspondence;

- **Communication data:** details of the support ticket;
- **System and application access data and internet and electronic network activity information:** system ID, LAN ID, email account, instant messaging account, mainframe ID, system passwords, Internet or other electronic network activity information (access logs, activity logs, electronic content produced using our systems);
- **Technical data:** Internet connectivity data, Internet protocol (IP) address, operator and carrier data, login data, browser type and version, device type, category and model, time zone setting and location data, language data, application version and SDK version, browser plug-in types and versions, operating system and platform, diagnostics data, such as crash logs and any other data we collect for the purposes of measuring technical diagnostics, transaction history, balances, user settings;
- **Cookies and geolocation data:** we may use cookies and other technologies to analyse our Site. If you want to know more about how we use cookies and what other information we may collect, please visit our Cookie Notice;
- **Analytics data:** event behavior analytics, pixel from social media;
- **Email address, content of notifications**;
- **Email addresses, content of email marketing messages:** upon receiving consent from you, we will share with you our marketing and promotional materials via email. You can always opt out of this by clicking the appropriate button in our emails to you. The withdrawal of your consent will not affect the lawfulness of processing based on consent before;
- **Marketing and research information:** identifiers (IP address, social media handle or other online identifiers, email address/mobile number, name and address), demographic data (income, family status, age, gender, interests, pets, home ownership, health, current service providers), browser/web history data, preferences expressed through selection/viewing/purchase of goods, services, and content, mobile device information (type of device, device identification number, mobile operating system), social media content (blogs, posts, and anything posted online or that references an individual), analytics and profiles based on collected data, voice-enabled services.

Sources of Personal Data

We obtain personal data from such sources:

- **Data subjects themselves:** customers of our services and users of the Site, B2C customers or company representatives, namely owners and/or directors;
- **Partner service providers:** data collected by partners handling payment processing, cloud hosting, customer support, and blockchain analytics;
- **Public blockchain:** we obtain personal data from public blockchains, including transaction details and wallet addresses.

Purposes and Legal Bases for Processing Personal Data

Our wallet service allows you to store, transfer, and manage your virtual assets, (e.g., Bitcoin, Ethereum), buy virtual assets with fiat money, and sell virtual assets with the receipt of fiat money. Your wallet balance will include crypto funds, and you can perform various actions, such as opening cards, depositing funds, issuing a payment card, conversion between fiat and cryptocurrency, transfers, withdrawals. Please refer to our Terms of Use for more information on the services we provide.

All of these actions are subject to the regulatory requirements we must follow, and we will verify your identity through our KYC/KYB procedures as outlined below.

We process your personal data for the following purposes, based on the legal grounds set forth under GDPR:

Purposes for Processing Personal Data	Legal Bases
Account Creation and Management: to create and manage your user account, verify your identity, and provide you with access to the card wallet services	Contractual Necessity
Transaction Processing: to facilitate purchases, transfers, top-ups, withdrawals, and other financial activities related to your card wallet, including cryptocurrency or fiat transactions; this also includes linking third-party payment methods	Contractual Necessity, Legitimate Interests
Card Issuance Management: to issue virtual and physical cards linked to your wallet, and collect card-specific information (e.g., card numbers, expiration dates, security codes) to ensure proper functionality and security	Contractual Necessity, Legitimate Interests
Compliance with Legal Obligations: to fulfill legal requirements, including Know Your Customer (KYC), Know Your Business (KYB) procedures, anti-money laundering (AML), tax reporting, and other regulatory obligations	Legal Obligation
Fraud Prevention and Security: to detect, prevent, and investigate fraudulent activities, unauthorised access, or any activities that may harm our services or users	Legitimate Interests, Contractual Necessity
Customer Communication: to send account-related updates, transaction alerts, customer service messages, and marketing communications (if you have opted in)	Contractual Necessity, Legitimate Interests, Consent
Service Improvement: to monitor platform performance, improve user experience, conduct analytics, and develop new features	Legitimate Interests

Resolving Complaints and Technical Issues: to investigate and address user complaints and technical issues, involving data such as transaction records, communications, error logs, and system data to identify and resolve problems	Contractual Necessity, Legitimate Interests
Customer Due Diligence: to perform checks required by law, including KYC, KYB, AML checks, fraud prevention, and sanctions checks, to ensure compliance with regulatory obligations	Legal Obligation, Legitimate Interests
Monitoring Transactions and Activity: to monitor and analyse transactions for suspicious activities, detect fraud or money laundering, and ensure the security of your account and transactions	Legal Obligation, Legitimate Interests
Monitoring Use of Systems: to monitor and analyse your use of our platform, including the website, apps, and tools, to improve performance, detect issues, and optimise user experience	Legitimate Interests
Business Performance and Analytics: to conduct product and business analyses, evaluate effectiveness, identify trends, and make data-driven decisions to improve services based on user data and feedback	Legitimate Interests, Consent
Sending Essential Notifications: to inform you about transaction statuses, account updates, and other critical service-related information, such as successful payments, transfers, or card-related updates	Contractual Necessity
Marketing Communications: to send marketing messages about products, services, or promotions, with your consent, and to allow you to opt-out at any time	Consent
Marketing Products and Services: to use your data for understanding preferences, segmenting users, and marketing new products, services, or features of our platform	Legitimate Interests
Identification Verification: to verify your identity as part of account creation, KYC/KYB, fraud prevention, and legal compliance, including uploading and verifying ID and proof of address documentation	Explicit Consent, Legal Obligation, Contractual Necessity

If you are a resident of the Republic of Kazakhstan, we process your personal data for the above purposes, based on your consent and/or the legal grounds set forth above.

Customer Due Diligence and KYC/KYB Checks

We implement a KYC/KYB procedure as part of our commitment to preventing fraud, complying with AML regulations, and ensuring the security of your account. This procedure is also a legal requirement under financial regulations.

This includes:

- Verifying your identity through government-issued documents (e.g., passport, ID card);
- Conducting PEP checks to ensure compliance with financial regulations;
- Performing risk-scoring on transactions to assess the potential for fraudulent or illegal activity;
- Cross-checking sanctions lists to ensure compliance with international regulations.

These checks are conducted to ensure the security and compliance of our services and to fulfill our legal obligations.

KYC/KYB refers to the process of verifying your identity before you can fully access our card wallet services. As part of the KYC/KYB procedure, we may request the following information:

- A government-issued ID (e.g., passport, national ID card, driver's license);
- A selfie or photo of you holding your ID (for verification purposes);
- Proof of address (e.g., utility bill, bank statement) to confirm your residential address.

SumSub: We have partnered with SumSub, the trusted third-party provider, to handle our KYC/KYB process. SumSub offers secure identity verification services to help us efficiently and accurately verify your identity in compliance with AML/KYC/KYB regulations.

When you begin the KYC/KYB process, your personal data (including identity documents) will be securely transferred to SumSub, who will verify the documents for compliance with AML and fraud prevention regulations.

Once SumSub successfully verifies your identity, we will process the information accordingly, allowing you to fully access the card wallet services.

For more information on how SumSub handles your data, please refer to their Privacy Notice.

How We Share Your Personal Data

We may share your personal data with the following parties:

- **Service Providers:** we work with third-party service providers (listed below) who assist in processing transactions, hosting, analytics, customer support, fraud detection, and marketing. These providers have access to your personal data only to the extent necessary to perform their services;

- **SumSub (KYC/KYB Verification):** for KYC/KYB and identity verification, your personal data is securely transferred to SumSub. They will handle the verification process in compliance with regulatory requirements;
- **Regulatory and Law Enforcement Authorities:** we may disclose your personal data to comply with legal obligations, such as reporting to financial regulatory bodies or responding to subpoenas or court orders;
- **Business Partners:** we may share data with trusted partners for marketing purposes (with your consent), or as part of a business transaction (e.g., in the event of a merger or acquisition);
- **Affiliates:** for purposes of including operational efficiency, marketing, customer support, legal compliance, and business management, with appropriate safeguards in place to protect your data;
- **Other Users:** in the case of transactions or transfers, some of your data (such as transaction details) may be visible to other parties involved in the transaction.

Your personal information may be shared with the following categories of third-party service providers:

- Identity authentication service providers;
- Software development service providers;
- Identity verification service providers;
- Contractors service providers;
- Tax & accounting software tools;
- Email marketing service providers;
- Cloud computing service providers;
- Productivity & collaboration tools;
- Blockchain analytics service providers;
- Messaging & communication service providers;
- Customer support software tools;
- Payment processing service providers;
- Web analytics tools;
- Social media service providers;
- Web analytics tools.

The providers listed above process your information based on our instructions only.

As part of providing our services, your personal data may be transferred to, and stored in, countries outside the European Economic Area (EEA), including countries that may not have the same data protection laws as your home country. If we transfer your data outside the EEA, we ensure that appropriate safeguards are in place to protect your data, including using Standard Contractual Clauses as adopted by the European

Commission or ensuring that the recipient country provides adequate data protection. Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

By using the services of Hardline Holdings Limited, the users from the Republic of Kazakhstan hereby give their explicit consent to any transfers of their personal data to other countries, as outlined in this Notice and in accordance with the terms and purposes described herein.

Other disclosures

In addition to the disclosures for the purposes identified before, we may disclose information about you for the following purposes:

- **Law enforcement, legal process and compliance:** if we are required to do so by law, in connection with any legal proceedings or to establish, exercise or defend our legal rights, or in the good-faith belief that such action is necessary to comply with applicable laws, in response to a facially valid court order, judicial or other government subpoena or warrant, or to otherwise cooperate with law enforcement or other governmental agencies. We also reserve the right to disclose personal data or other information that we believe, in good faith, is appropriate or necessary to: (i) take precautions against liability; (ii) protect ourselves or others from fraudulent, abusive, or unlawful uses or activity; (iii) investigate and defend ourselves against any third-party claims or allegations; (iv) protect the security or integrity of our services and any facilities or equipment used to make our services available; or (v) protect our property or other legal rights, enforce our contracts, or protect the rights, property, or safety of others;
- **Change of ownership or other business needs:** (i) in case we sell, licence or otherwise assign our company, corporate rights, the Site or its separate parts or features to third parties; (ii) as part of a transaction, financing, or for other business needs (e.g., if we need to disclose your personal data to the prospective lender or bank, investor or prospective investor, and/or their professional advisers as part of certain due diligence processes, as the case may be); (iii) we may also disclose and otherwise transfer your personal data to an acquirer, successor or assignee as part of any merger, acquisition, debt financing, sale of assets, or similar transaction, as well as in the event of an insolvency, bankruptcy, or receivership in which information is transferred to one or more third parties as one of our business assets and only if the recipient of the information commits to a privacy policy that has terms substantially consistent with this Notice.

Data Retention

We will retain your personal data for as long as necessary to fulfill the purposes outlined in this Notice or to comply with legal obligations. Specifically:

- **Transaction Data:** we will retain transaction records for a period of 5 years, in accordance with tax, AML, accounting and other legal obligations;

- **Account Data:** we will retain your account data for as long as you maintain an active account with us. If you close your account, we may retain certain information for a period necessary to comply with our legal obligations (e.g., AML/KYC/KYB regulations);
- **Marketing Data:** if you have opted in to receive marketing communications, we will retain your email address and preferences until you withdraw consent.

Once your data is no longer needed, we will either delete or anonymise it.

Please note that certain personal data cannot be removed or deleted at all because of the nature of the blockchain. The blockchain technology used in the provision of our services operates on a decentralised network, where transactions are recorded in an immutable and transparent manner. This characteristic ensures the integrity and security of the data stored on the blockchain. However, it also means that once data is added to the blockchain, it becomes virtually impossible to remove or delete it.

Your Rights

You may exercise GDPR rights regarding your personal data. In particular, you have the right to:

- **The right to access your information**.

  You have the right to know what personal data we process. As such you can obtain the disclosure of the personal data involved in the processing and you can obtain a copy of the information undergoing processing.

- **The right to verify your information and seek its rectification**.

  If you find that we process inaccurate or out-of-date information, you can verify the accuracy of your information and/or ask for it to be updated or corrected;

- **The right to have your personal data deleted**.

  If we are not under the obligation to keep your personal data for legal compliance and it is not needed in the scope of an active contract or claim, we will remove your information upon your request.

- **The right to restrict the processing of your information**.

  When you contest the accuracy of your information, believe we process it unlawfully or want to object to the processing, you have the right to temporarily stop the processing of your information to check if the processing was consistent. In this case, we will stop processing your personal data (other than storing it) until we are able to provide you with evidence of its lawful processing.

- **The right to have your personal data transferred to another organisation.**

  Where we process your personal data on the legal basis of consent you provided us or on the necessity to perform a contract, we can make, at your request, your personal data available to you or to an organisation of your choosing.

- **The right to object against the processing of your information**.

If we process your information for our legitimate interests (e.g., for direct marketing emails or for our marketing research purposes), you can object to it. Let us know what you object against and we will consider your request. If there are no compelling interests for us to refuse to perform your request, we will stop the processing for such purposes. If we believe our compelling interests outweigh your right to privacy, we will clarify this to you.

- **The right to withdraw consent.**

  If we process your personal data based on your consent, you can withdraw it at any time.

You can formulate such requests or channel further questions on data protection by contacting us directly at support@kolo.xyz, or by contacting our DPO at: kolo.dpo@legalnodes.com.

If you believe that our use of personal information violates your rights, or if you are dissatisfied with a response you received to a request you formulated to us, you have the right to lodge a complaint with the competent data protection authority of your choice.

If you are a resident of the Republic of Kazakhstan, you may withdraw your consent to the processing of your personal data in accordance with paragraph 1 of Article 24 of the Law of the Republic of Kazakhstan dated May 21, 2013 No. 94-V “On Personal Data and Their Protection” by submitting a written request to the address of Hardline Holdings Limited’s location, to its email address support@kolo.xyz. You may not withdraw your consent for the collection and processing of personal data in cases where such withdrawal would contradict the laws of the Republic of Kazakhstan or if there is an outstanding obligation. In the event that you withdraw your consent, Hardline Holdings Limited is entitled to continue processing your personal data without your consent if there are grounds specified in Article 9 of the Law of the Republic of Kazakhstan dated May 21, 2013 No. 94-V “On Personal Data and Their Protection”.

Data Security

We take the security of your personal data seriously and implement a variety of technical and organisational measures to protect it. In particular, we have implemented:

- Data encryption (both in transit and at rest);
- KYC/KYB authentication for account access;
- Secure servers and firewalls;
- Regular security audits and vulnerability assessments.

We take all necessary measures to protect your information from unauthorised or accidental access, destruction, modification, blocking, copying, and distribution, as well as from other illegal actions of third parties. As we use the services of third-party software providers across several countries outside of the European Union, we may transfer the collected information to those countries for further processing. In such

cases, we will make sure that relevant safeguards are in place. More information on such safeguards can be provided upon request.

We also make sure that access to your information stored in our database is only possible via a secure and closed VPN connection. Additionally, all communications exposed to the internet are TLS encrypted to provide the highest level of communications security.

Changes to this Notice

We may update this Notice from time to time by posting a new version on our Site. We advise you to check this page occasionally to ensure you are happy with any changes. However, we will endeavour to provide you with an announcement about any significant changes.