

PRIVACY POLICY

Aurumverse LLC

Effective Date: July 21, 2026

This Privacy Policy explains how Aurumverse LLC and the applicable entities operating the Aurumverse ecosystem (collectively, "Aurumverse," "we," "us," or "our") collect, use, disclose, retain, transfer, and protect Personal Information when you visit, access, or use our websites, decentralized application interfaces, Realone marketplace, account and investor portals, project pages, token-related features, communications channels, creator or referral programs, and related online or offline services (collectively, the "Platform").

This Privacy Policy should be read together with the Terms of Use, KYC / AML Consent, Electronic Communications Consent, Risk Disclosures, Token Terms, project memorandums, subscription agreements, offering documents, cookie or consent notices, and any transaction-specific notices made available to you. If a project-specific notice conflicts with this Privacy Policy for a particular processing activity, the more specific notice will control for that activity to the extent permitted by law.

1. Scope

This Privacy Policy applies to Personal Information processed through the Platform, including when you browse a public page, create or use an account, connect a compatible wallet, complete identity or eligibility checks, access project materials, acquire or redeem RTOKEN, acquire an RP-Series token, use a supported peer-to-peer listing function, communicate with us, join a community channel, respond to marketing, or arrive through a creator, affiliate, or referral link.

It does not govern a third party's independent handling of information through a wallet application, public blockchain, exchange, blockchain explorer, payment or stablecoin provider, identity verification provider, social network, messaging service, website, or other service that we do not control. Those parties may act as independent controllers and apply their own terms and privacy notices.

2. Who We Are and Our Privacy Roles

Aurumverse LLC is the primary organization responsible for this Privacy Policy. Depending on the service or project, an affiliate, Realone, a project entity, an asset-owning or operating entity, or another identified party may also determine why and how certain Personal Information is processed. That party may act as a separate controller or, where applicable, a joint controller. Any materially different role will be explained in the relevant project or transaction documents.

Service providers that process Personal Information only on our instructions generally act as processors or service providers. Public blockchain participants, wallet providers, exchanges, and other independent services normally determine their own processing and are not controlled by Aurumverse.

3. Key Definitions

Personal Information or Personal Data. Information about an identified or reasonably identifiable individual. It may include information that identifies you directly and information that becomes identifying when combined with other data.

Processing. Any operation involving Personal Information, including collection, recording, organization, storage, access, use, analysis, transmission, disclosure, restriction, deletion, anonymization, or destruction.

Usage Data. Technical and activity information generated when you use the Platform, such as IP address, device and browser data, timestamps, pages viewed, click paths, referral data, error logs, and security events.

Wallet Data. A public wallet address and associated public blockchain activity, transaction hashes, network information, authentication signatures, token balances or records, and smart-contract interactions.

User. Any visitor, account holder, wallet user, prospective or actual purchaser, subscriber, project participant, creator, referral partner, representative, or other person using or communicating with the Platform.

4. Personal Information We May Collect

4.1 Account and Contact Information

We may collect your name, email address, telephone number, country, province or state, mailing address, preferred language and communication method, account username, encrypted or hashed login credentials, authentication records, profile details, account status, communication preferences, and information you include in messages or support requests.

4.2 Identity, KYC, AML, Eligibility, and Compliance Information

Where required, we or an approved verification provider may collect or generate date of birth, nationality or residency, government-issued identification, photographs or liveness checks, proof of address, tax residency or identification numbers, corporate and beneficial ownership information, occupation or business information, source of funds or wealth information, investor or purchaser eligibility information, accreditation or classification information, sanctions and politically exposed person screening results, risk indicators, declarations, certifications, subscription forms, and supporting documents.

Some of this information is sensitive. It may be collected directly by a verification provider and made available to us as a verification result, risk result, or limited record rather than as a complete copy of the underlying document.

4.3 Wallet, Blockchain, and Smart-Contract Information

When you connect or use a wallet, we may process your public wallet address, applicable blockchain network, wallet type, connection or authentication event, transaction hash, timestamp, token acquisition, redemption, transfer, listing, cancellation or reward activity, RToken and RP-Series records, gas and network metadata, smart-contract interaction data, and other public information associated with the wallet address.

Aurumverse does not need your wallet private key or seed phrase to operate the Platform. You should never provide a private key or seed phrase to Aurumverse, our support personnel, a creator, or any person claiming to represent us.

4.4 Stablecoin, Token, Subscription, and Project Information

We may process information relating to USDT, USDC, RTOKEN, and RP-Series activity; wallet-to-platform or platform-to-wallet transfers; acquisition or redemption requests; transaction identifiers; internal ledger entries; pricing or conversion records; fees; refunds or failed transactions; project interests; document access; subscription agreements; acknowledgements; eligibility representations; voting or governance activity; and communications concerning a project or transaction.

4.5 Creator, Affiliate, and Referral Information

If you enter through a creator, affiliate, campaign, or referral link, we may collect a campaign or partner identifier, referring URL, click timestamp, cookie or similar identifier, IP address, device and browser information, landing-page activity, account registration, KYC status, eligible purchase confirmation, transaction amount where needed to calculate an agreed commission, attribution period, fraud or duplicate-account indicators, and commission validation records.

If you participate as a creator or referral partner, we may also collect your name, business and contact details, social-media profiles, audience information, content and communications, tax or payment information, wallet address for permitted payments, contract and commission terms, referral performance, disclosure compliance, and payment history.

4.6 Technical, Device, Cookie, and Usage Information

We and our providers may automatically collect IP address, approximate location derived from IP, browser type and version, device and operating-system information, language, time zone, referring source, pages and documents viewed, buttons or links selected, session duration, request and response metadata, cookie or local-storage identifiers, performance metrics, crash and error logs, diagnostic records, and security events.

4.7 Communications, Support, Community, and Marketing Information

We may collect emails, calls, support messages, Telegram or WhatsApp interactions, community participation, chat or conversation history, attachments, feedback, complaints, survey responses, marketing consent, unsubscribe records, campaign engagement, event participation, and information you make available when interacting with our official social-media accounts.

5. How We Obtain Personal Information

We obtain Personal Information from you, from your authorized representative, automatically through the Platform, from public blockchain records, from project and transaction entities, from verification and compliance providers, from wallet or infrastructure providers, from creators and referral partners, from communications and support platforms, from analytics and security providers, and from public or commercially available sources where permitted by law.

If you provide Personal Information about another person, you represent that you are authorized to do so and that you have given that person any notice required by law.

6. How We Use Personal Information

We may use Personal Information for the following purposes:

- to provide, maintain, administer, and improve the Platform, websites, DApp interfaces, Realone marketplace, accounts, project pages, and supported functions;
- to create and authenticate accounts, connect public wallet addresses, display supported balances and activity, and maintain records of RTOKEN and RP-Series transactions;
- to provide access to project materials, process subscriptions and eligible transactions, manage requests, and deliver notices or confirmations;
- to conduct KYC, AML, sanctions, eligibility, fraud, cybersecurity, source-of-funds, and other legal or risk reviews;
- to reconcile on-chain and off-chain activity, maintain internal ledgers, investigate errors, prevent duplicate or unauthorized transactions, and support audits;
- to operate creator, affiliate, and referral programs, attribute users or eligible purchases, calculate commissions, prevent self-referral or manipulation, and resolve attribution disputes;
- to communicate with you, answer inquiries, provide customer support, manage community channels, and send security, legal, compliance, transaction, or project notices;
- to analyze usage, improve functionality and content, measure campaign performance, and conduct marketing or advertising where permitted by law;
- to protect users, our entities, our partners, and the Platform; enforce agreements; establish, exercise, or defend legal claims; and respond to lawful requests; and
- to create aggregated, anonymized, or de-identified information for lawful analytics, research, security, reporting, and business planning.

7. Consent and Other Legal Bases

We collect, use, and disclose Personal Information with consent or under another legal authority available in the applicable jurisdiction. Consent may be express or implied depending on the sensitivity of the information, your reasonable expectations, and the circumstances. You may withdraw consent where permitted, but withdrawal does not affect earlier lawful processing and may prevent us from providing an account, project access, a transaction, or another requested service.

For users in the European Economic Area or United Kingdom, we rely on one or more of the following legal bases as appropriate: consent; steps requested before entering into a contract or performance of a contract; compliance with a legal obligation; and our or a third party's legitimate interests where those interests are not overridden by your rights and freedoms. Legitimate interests may include operating and securing the Platform, preventing fraud, maintaining records, responding to inquiries, improving services, and managing business relationships. Where required, we conduct the appropriate balancing assessment.

Where processing involves sensitive information, criminal-offence information, biometric verification, or another specially protected category, we will rely on an additional condition or authorization where required by law.

8. KYC, AML, Eligibility, and Fraud Screening

Access to certain Platform features or project opportunities may require identity, eligibility, sanctions, source-of-funds, or other compliance checks. We may use third-party verification providers, public and commercial databases, and risk-screening tools to perform these checks. We may retain evidence that a check occurred, the result, relevant risk indicators, and supporting records needed to satisfy legal, audit, dispute, or security requirements.

We may decline, delay, restrict, suspend, or refer an account or transaction for manual review where verification is incomplete, information is inconsistent, a risk threshold is met, or law or policy requires additional review. We will not disclose information that would compromise a fraud, AML, sanctions, security, or legal investigation.

9. Public Blockchain and Wallet Notice

Public blockchain networks are designed to make transaction data broadly visible and durable. Wallet addresses, transaction amounts, token transfers, contract interactions, timestamps, hashes, and related activity may be publicly searchable and may be copied, analyzed, or associated with other information by third parties.

Aurumverse may associate a public wallet address with an account, identity-verification record, transaction history, project activity, creator attribution, or support communication when necessary to operate the Platform, prevent fraud, maintain accurate records, or comply with law. Information recorded on a public blockchain is maintained by a decentralized network rather than by Aurumverse. We generally cannot erase, reverse, conceal, or amend on-chain records. Where a valid privacy request applies, we will address Personal Information within systems we control, subject to legal and technical limitations, but the public blockchain record may remain available.

10. Cookies and Similar Technologies

We may use session cookies, persistent cookies, pixels, software development kits, local storage, referral identifiers, and similar technologies to keep you signed in, remember preferences and consent choices, secure the Platform, detect abuse, understand use, diagnose performance, attribute creator or advertising referrals, and measure campaign effectiveness.

Where required, non-essential analytics, advertising, or referral technologies will be used only after consent. You may manage available choices through a cookie banner, privacy settings, browser controls, device settings, or an opt-out mechanism. Blocking certain technologies may affect account access, wallet connection, transaction security, attribution, or other functionality. Browser-based deletion of a referral cookie may prevent a purchase from being attributed to a creator or partner.

11. Automated Tools and Profiling

We may use automated tools to support fraud detection, cybersecurity monitoring, sanctions and identity screening, duplicate-account detection, marketing measurement, referral attribution, and risk prioritization. These tools may generate indicators or recommendations for review.

Unless we specifically tell you otherwise, we do not intend to make a decision that produces legal or similarly significant effects solely through automated processing without appropriate safeguards.

Where applicable law gives you a right to information about or human review of an automated decision, you may contact us using Section 24.

12. How We Disclose Personal Information

We may disclose Personal Information only as reasonably necessary for the purposes described in this Privacy Policy, including to:

- affiliates, Realone, project entities, asset-owning or operating entities, and other parties identified in applicable transaction documents;
- KYC, AML, sanctions, identity, eligibility, fraud, cybersecurity, and compliance providers;
- cloud hosting, database, content-delivery, authentication, wallet-connection, blockchain infrastructure, analytics, error-monitoring, and technical support providers;
- communication, email, CRM, customer-support, Telegram, WhatsApp, community, and social-media service providers;
- creator, affiliate, referral, landing-page, campaign-measurement, and commission-administration providers and partners, limited to information needed for attribution, validation, payment, and dispute resolution;
- banks, stablecoin or payment providers, accountants, auditors, insurers, legal counsel, tax advisers, consultants, and other professional advisers;
- regulators, courts, law-enforcement agencies, governmental bodies, counterparties, and other persons when disclosure is required or permitted by law or reasonably necessary to protect rights, safety, security, or property;
- a buyer, investor, lender, successor, or adviser in connection with an actual or proposed financing, reorganization, merger, sale, transfer, insolvency, or similar business transaction, subject to appropriate safeguards; and
- another party at your direction or with your consent.

We do not sell Personal Information for money in the ordinary course of business. Certain advertising or analytics disclosures may be considered a "sale" or "sharing" under some U.S. state laws even when no money is exchanged. Where those laws apply, we will provide the notices and opt-out methods they require.

13. International Processing and Transfers

Aurumverse, its affiliates, project entities, service providers, blockchain infrastructure, and counterparties may operate in Canada, the United States, and other jurisdictions. As a result, Personal Information may be accessed, stored, or processed outside your province, state, or country and may be subject to lawful access by authorities in those jurisdictions.

Where required for EEA or UK Personal Data, we use an applicable transfer mechanism, such as an adequacy decision, standard contractual clauses, the UK international data transfer addendum or agreement, or another legally recognized safeguard or exception. You may contact us for information about safeguards that apply to a specific transfer, subject to legal and confidentiality limits.

14. Data Retention

We retain Personal Information only for as long as reasonably necessary for the purposes described in this Privacy Policy and to meet legal, tax, accounting, securities, AML, sanctions, audit, contractual, dispute-resolution, fraud-prevention, and security requirements. The applicable period depends on the type and sensitivity of the information, the nature of the relationship or transaction, the risk of harm, and the law that applies.

Account, transaction, KYC, subscription, creator-attribution, commission, and compliance records may need to be retained after an account is closed or a transaction is completed. When retention is no longer justified, we will take reasonable steps to delete, anonymize, restrict, or securely dispose of information within systems we control. Backups may be isolated and removed through normal retention cycles. Public blockchain data may remain permanently available and is outside our control.

15. Security

We use reasonable administrative, technical, organizational, and physical safeguards appropriate to the sensitivity of the information. Measures may include access controls, role-based permissions, encryption in transit and where appropriate at rest, authentication, logging and monitoring, vendor review, secure infrastructure, incident response, backups, personnel controls, and internal policies.

No website, internet transmission, database, wallet, smart contract, or blockchain network is completely secure. You are responsible for protecting your device, account credentials, wallet, private keys, seed phrases, recovery information, and authentication methods. Notify us promptly if you believe an Aurumverse account or communication channel has been compromised.

16. Your Privacy Rights and Choices

Depending on where you live and the law that applies, you may have some or all of the following rights:

- to be informed about our collection, use, disclosure, and retention of Personal Information;
- to request confirmation of processing and access to Personal Information we hold about you;
- to request correction of inaccurate or incomplete Personal Information;
- to withdraw consent, subject to legal or contractual restrictions and reasonable notice;
- to request deletion, anonymization, restriction, or blocking of eligible information;
- to object to certain processing, including direct marketing or processing based on legitimate interests;
- to request portability of eligible information in a structured, commonly used format;
- to opt out of certain targeted advertising, sale, or sharing where applicable;
- to request information about or review of certain automated decisions; and
- to complain to Aurumverse or an applicable privacy or data-protection authority.

To protect accounts and Personal Information, we may verify your identity and authority before acting on a request. We may ask for information sufficient to match you to our records. An authorized agent may submit a request where permitted, but we may require proof of authority and direct identity verification. Rights are subject to exceptions, including obligations relating to AML,

sanctions, securities, tax, accounting, fraud, cybersecurity, legal claims, and public blockchain limitations.

We will not unlawfully discriminate against you for exercising a privacy right. We normally do not charge a fee, but may charge a reasonable fee or decline a request where permitted by law if it is manifestly unfounded, excessive, repetitive, or impossible to verify.

17. Additional Information for Canadian Users

Where Canadian private-sector privacy law applies, we follow applicable requirements concerning accountability, identified purposes, meaningful consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access, and the ability to challenge compliance. You may ask to access or correct Personal Information and may withdraw consent where permitted. If you are not satisfied with our response, you may have the right to complain to the Office of the Privacy Commissioner of Canada or the applicable provincial privacy authority.

18. Additional Information for EEA and UK Users

If the EU GDPR or UK GDPR applies, the controller for the relevant processing is Aurumverse LLC or the other entity identified at collection or in the applicable project documents. Subject to legal conditions and exceptions, you may request access, rectification, erasure, restriction, portability, or objection; withdraw consent at any time for future processing; and complain to the supervisory authority where you live, work, or believe an infringement occurred. For the United Kingdom, this may include the Information Commissioner's Office.

If we are required to appoint an EEA or UK representative or data-protection officer for a particular activity, the applicable contact information will be made available through the Platform or the relevant notice.

19. Additional Information for California and Other U.S. State Residents

If a U.S. state privacy law applies to Aurumverse and to your information, you may have rights to know, access, correct, delete, or obtain a copy of Personal Information; to opt out of certain sale, sharing, targeted advertising, or qualifying profiling; to limit certain uses of sensitive Personal Information; and to appeal a denied request. The categories of Personal Information we may collect and disclose are described in Sections 4 and 12, and the business purposes are described in Section 6.

We use sensitive Personal Information, such as government-identification and source-of-funds information, for identity verification, KYC/AML, security, fraud prevention, legal compliance, and other permitted operational purposes. We do not use it to infer characteristics about you unless separately disclosed and permitted by law. Where required, we will honor a valid opt-out preference signal, such as Global Privacy Control, for the browser or device from which the signal is sent.

We do not knowingly offer a financial incentive in exchange for a consumer's Personal Information unless we provide the separate notice and obtain the agreement required by law. Creator or referral commissions are compensation for contracted promotional services and attribution, not payment to a referred user for that user's Personal Information.

20. Marketing and Electronic Communications

Where permitted by law, we may send information about Aurumverse, Realone, platform updates, project opportunities, educational materials, events, or related services. We obtain consent where required and maintain records of consent and unsubscribe requests. You may unsubscribe from marketing emails using the link in the message or by contacting us. We may still send non-marketing communications, such as security alerts, legal notices, KYC requests, account messages, transaction confirmations, project notices, and policy updates.

21. Children and Age Restrictions

The Platform is not intended for anyone under 18 or under the age of legal majority in the person's jurisdiction, whichever is higher. We do not knowingly collect Personal Information from a child for use of the Platform. If we learn that a child provided Personal Information without valid authorization, we will take reasonable steps to delete or restrict it, subject to legal and technical limitations.

22. Third-Party Links, Wallets, and Services

The Platform may link to or integrate third-party wallets, exchanges, blockchain explorers, identity providers, stablecoin or payment services, social networks, messaging platforms, analytics services, creator platforms, and websites. A link or integration does not mean that Aurumverse controls or endorses the third party's privacy or security practices. Review the third party's privacy notice and terms before providing information or connecting an account or wallet.

23. Changes to This Privacy Policy

We may update this Privacy Policy to reflect changes in the Platform, projects, technology, service providers, legal requirements, or business practices. The effective date at the top identifies the current version. If a change is material, we may provide additional notice through the Platform, email, an account message, or another reasonable channel. Your continued use after the effective date is subject to applicable law and any consent requirement.

24. Contact Us and Submit a Privacy Request

To ask a question, exercise a privacy right, request information about an international transfer, or make a complaint, contact:

Organization: Aurumverse LLC

Website: <https://aurumverse.io>

Email: admin@aurumverse.io

Subject line: Privacy Request

Please describe your request and identify the account email or wallet address relevant to the request, but do not send a password, private key, seed phrase, or unnecessary identity document by ordinary email. We will respond within the period required by applicable law and may provide a secure method for identity verification or document transfer.