BALDIVICIO & CO.

Privacy Policy

Effective Date: April 13, 2026

This Privacy Policy ("Policy") explains how Baldivicio collects, uses, stores, shares, retains, and otherwise processes personal information in connection with Baldivicio's website, mobile application, custodial wallet functionality, customer support operations, legal disclosures, compliance processes, and related services.

Baldivicio is a digital financial services platform made available primarily through its mobile application. Baldivicio currently supports USDC-only activity on Ethereum Mainnet through a custodial model. Certain fiat-to-digital-asset and digital-asset-to-fiat services connected to the Baldivicio experience may be provided in whole or in part by third-party providers, including Banxa.

Because Baldivicio operates in a regulated, security-sensitive, and blockchain-connected environment, it may process a broad range of information relating to identity, onboarding, account activity, device and access signals, wallet activity, compliance screening, customer support, legal obligations, and service operations.

Please read this Policy carefully. It should be read together with Baldivicio's Terms of Service, Acceptable Use Policy, Deposit Insurance Disclosure, Reserve and Transparency Attestation, Customer Identification Program Notice, E-Sign Consent and Electronic Communications Agreement, Fee Schedule and Schedule of Charges, Irreversible Transactions Disclosure, System Outage and Degradation Policy, Account Suspension, Freezing, and Closure Policy, and any other notices or disclosures made available through Baldivicio.

By accessing Baldivicio, applying for an account, using the mobile application, interacting with customer support, or otherwise engaging with services covered by this Policy, you acknowledge that you have read and understood this Policy.

1. Scope of This Policy

This Policy applies to personal information processed by Baldivicio in connection with:

- the Baldivicio mobile application;
- the public Baldivicio website and related pages where this Policy is referenced;
- account onboarding, verification, activation, use, suspension, review, closure, and related lifecycle management;
- custodial wallet and supported USDC activity on Ethereum Mainnet;
- customer support, complaint handling, and service communications;
- compliance, fraud prevention, sanctions screening, legal review, security monitoring, and investigations; and
- interactions involving third-party services that are connected to the Baldivicio experience, where Baldivicio receives or processes related information.

This Policy does not necessarily govern the privacy practices of third-party services that have their own privacy policies, terms, or notices, even where those services are linked from, integrated with, or made

available alongside Baldivicio. If you interact directly with a third-party provider, that provider's own terms and privacy practices may also apply.

2. Key Service Context

Baldivicio is not a traditional chartered bank or depository institution. It operates through a custodial model in which Baldivicio holds and manages private keys associated with supported wallet functionality on behalf of users. Users do not receive or export private keys.

Baldivicio currently supports USDC on Ethereum Mainnet only. Because Baldivicio's services interact with blockchain infrastructure and, in some cases, third-party providers such as Banxa, privacy expectations may differ in important ways from those associated with a conventional financial account or a purely off-chain application.

For example, certain transaction-related data may also exist on a public blockchain, may be visible to third parties, and may remain visible indefinitely. Likewise, certain funding, payout, conversion, settlement, or verification-related events may involve information flows between Baldivicio and third-party providers operating under their own obligations and systems.

3. Information We Collect

Baldivicio may collect information directly from you, automatically through your use of the service, from blockchain and transaction activity, from service providers and business partners, from public or regulatory sources, and from other lawful sources.

The categories of information Baldivicio may collect include the following.

3.1 Information You Provide Directly

When you apply for an account, use the service, contact support, or otherwise interact with Baldivicio, you may provide information such as your name, date of birth, residential address, email address, phone number, nationality, account credentials, government-issued identification details, source-of-funds information, source-of-wealth information, occupation or employment information, expected account activity information, declarations relevant to sanctions or politically exposed person screening, statements or explanations you submit during review, and correspondence you send to Baldivicio.

You may also provide transaction instructions, destination details, support requests, dispute information, closure requests, account recovery information, feedback, and other content you choose to submit in connection with the service.

3.2 Identity Verification and Compliance Information

To support lawful onboarding, ongoing compliance, fraud prevention, account security, and risk management, Baldivicio may collect or generate information used to verify identity and assess eligibility or risk. This may include copies of identification documents, information extracted from those documents, proof-of-address materials, verification results, screening matches, onboarding decisions, escalation flags, enhanced review notes, manual review outputs, watchlist or sanctions screening results, and related compliance records.

Baldivicio may also collect or derive information needed to determine whether an account should be approved, restricted, reviewed further, suspended, frozen, or closed.

3.3 Account and Profile Information

Baldivicio may collect information associated with your account setup and ongoing use, including account identifiers, profile details, user preferences, communication preferences, authentication events, account

status history, service feature usage, statement requests, proof-of-account requests, and records relating to account restriction, review, suspension, or closure.

3.4 Transaction and Wallet Activity Information

Because Baldivicio provides custodial wallet functionality tied to supported USDC activity on Ethereum Mainnet, Baldivicio may collect and process information such as wallet addresses, destination addresses, source addresses, transaction hashes, transaction timestamps, amounts, blockchain confirmations, on-chain status, transaction instructions, pending and completed transfer records, inbound and outbound transfer data, operational notes relating to transaction review, and records relating to whether a transaction was delayed, restricted, refused, completed, or later investigated.

Baldivicio may also process transaction-related metadata from internal controls and workflow systems, including state changes, review status, execution timing, routing data, and interactions between transaction activity and account restrictions or compliance measures.

3.5 Blockchain and Public-Ledger Information

Transactions involving blockchain-based assets may be recorded on public ledgers outside Baldivicio's direct control. As a result, Baldivicio may collect, observe, use, and analyze public blockchain information relevant to your use of the service, including wallet-address relationships, transaction histories, transfers into or out of relevant addresses, exposure to higher-risk destinations, public smart-contract interactions where relevant to risk review, and other publicly observable on-chain information.

Even where Baldivicio does not display all such data in the app, it may process public-ledger information for compliance, security, operations, dispute review, and fraud detection purposes.

3.6 Device, Access, Session, and Technical Information

When you access Baldivicio, Baldivicio may collect information relating to your device and your use of the service. This may include device identifiers, app version, operating system, browser or in-app webview information where relevant, IP address, approximate location information inferred from technical signals, login timestamps, session records, account access history, crash or error data, performance telemetry, network information, and other device or access signals reasonably necessary to operate, secure, monitor, and improve the service.

Baldivicio may also process technical and behavioral information to help detect suspicious access, account takeover risk, fraud, misuse, or attempts to evade compliance or security controls.

3.7 Customer Support and Communications Information

If you contact Baldivicio, respond to a review request, report suspected fraud, request account recovery, request closure, or otherwise communicate with Baldivicio, Baldivicio may collect your messages, attachments, account references, conversation history, support outcomes, escalation records, complaint details, dispute materials, and related service notes.

Baldivicio may also retain records of communications delivered to you, including in-app notices, emails, prompts, and support follow-up messages.

3.8 Information From Third-Party Providers and Partners

Baldivicio may receive information from third-party providers, vendors, service partners, or integrations that support the service. This may include identity-verification providers, compliance vendors, sanctions-screening providers, fraud-detection partners, analytics or infrastructure providers, support platforms, email or notification providers, and third-party providers connected to funding, payout, conversion, or settlement functions, including Banxa.

For example, where a service connected to Baldivicio involves Banxa or another third-party provider, Baldivicio may receive information such as order status, verification status, operational outcomes, payout or settlement status, exception codes, dispute or escalation signals, and other information reasonably necessary to support service delivery, risk management, user support, and recordkeeping.

3.9 Information From Public, Legal, and Regulatory Sources

Baldivicio may collect information from public records, sanctions and watchlist databases, regulators, government authorities, court filings, law-enforcement requests, public blockchain data, fraud or scam intelligence sources, cybersecurity threat intelligence feeds, and other lawful sources relevant to legal compliance, user safety, and service integrity.

4. How We Use Personal Information

Baldivicio may use personal information for a range of operational, legal, security, and service-related purposes. These uses include the following.

4.1 To Provide and Operate the Service

Baldivicio may use personal information to create and administer accounts, deliver the mobile application and related services, provide custodial wallet functionality, display supported balances, process supported transactions, support account lifecycle management, provide statements and records, send operational notices, respond to support requests, and otherwise make Baldivicio available to users in accordance with the service design.

4.2 To Verify Identity and Assess Eligibility

Baldivicio may use personal information to verify identity, evaluate onboarding applications, assess eligibility, confirm account ownership, support ongoing review, request additional documentation, and determine whether an account may be opened, maintained, restricted, suspended, or closed.

4.3 To Comply With Legal and Regulatory Obligations

Baldivicio may use personal information to comply with applicable law, legal process, regulatory obligations, sanctions obligations, financial crime prevention requirements, recordkeeping obligations, consumer-protection obligations, lawful disclosure requirements, and related compliance expectations.

This may include customer due diligence, watchlist screening, sanctions screening, politically exposed person screening, fraud review, suspicious activity review, internal investigations, regulatory reporting, legal preservation, and cooperation with competent authorities where permitted or required by law.

4.4 To Protect Users, Baldivicio, and the Broader Financial System

Baldivicio may use personal information to detect, prevent, investigate, and respond to fraud, scams, phishing, account takeover, cyber threats, sanctions evasion, money laundering, terrorist financing, misuse of the platform, suspicious transfers, destination risk, abuse of support channels, and other conduct that may threaten users, Baldivicio, counterparties, or the broader financial system.

4.5 To Secure the Service and Accounts

Baldivicio may use personal information to authenticate users, manage sessions, protect account access, detect suspicious sign-in activity, investigate unauthorized access, support account recovery, analyze device and access patterns, apply holds or restrictions, and maintain system integrity, resiliency, and security.

4.6 To Process and Review Transactions

Baldivicio may use personal information to receive transaction instructions, validate requests, review destinations, perform risk checks, process supported USDC activity, monitor pending and completed transfers, investigate transaction disputes, and enforce the Irreversible Transactions Disclosure, Account Suspension, Freezing, and Closure Policy, and other operational controls.

4.7 To Communicate With You

Baldivicio may use personal information to provide service-related communications, legal disclosures, account notices, onboarding or verification requests, security alerts, incident notices, support responses, policy updates, and other communications necessary or appropriate to operate the service.

4.8 To Improve, Maintain, and Develop the Service

Baldivicio may use personal information to diagnose outages, maintain infrastructure, analyze product usage, detect technical failures, prevent duplicate processing, improve the user experience, develop features, refine workflows, perform internal reporting, and improve operational efficiency, provided that such use is consistent with applicable law and this Policy.

4.9 To Establish, Exercise, or Defend Legal Rights

Baldivicio may use personal information to investigate claims, resolve disputes, enforce its agreements and policies, respond to legal complaints, preserve evidence, exercise defenses, pursue recoveries, or protect the rights, safety, and property of Baldivicio, its users, and others.

5. Legal Bases for Processing

Depending on the nature of the information, the context in which it is collected, and the law applicable to a particular user or processing activity, Baldivicio may process personal information on one or more of the following grounds:

- because the processing is necessary to provide the service you request or to take steps at your request before providing the service;
- because the processing is necessary to comply with legal or regulatory obligations;
- because the processing is necessary for Baldivicio's legitimate interests or the legitimate interests of users, partners, or the public, including interests in security, fraud prevention, compliance, service integrity, dispute handling, and product operations, where those interests are not overridden by applicable legal protections;
- because the processing is necessary to protect important interests, including the safety or security of users or the integrity of the platform; or
- because you have provided consent where consent is required or appropriate.

Where consent is relied upon under applicable law, you may have the right to withdraw that consent, although withdrawal does not affect the lawfulness of processing conducted before the withdrawal became effective and may affect whether Baldivicio can continue to provide some or all services.

6. How We Share Personal Information

Baldivicio does not sell personal information in the ordinary sense of exchanging it for money. However, Baldivicio may disclose personal information to third parties in a range of circumstances consistent with this Policy, applicable law, and the operation of the service.

Baldivicio may share personal information with the following categories of recipients.

6.1 Service Providers and Vendors

Baldivicio may share information with service providers that perform functions on Baldivicio's behalf, such as cloud hosting, infrastructure support, email delivery, analytics, identity verification, sanctions screening, fraud detection, compliance support, record storage, customer support tooling, security monitoring, and incident management.

These providers may be permitted to process personal information only as needed to provide services to Baldivicio, subject to contractual, legal, security, and confidentiality requirements as applicable.

6.2 Third-Party Financial or Operational Partners

Baldivicio may share information with third-party providers that support aspects of funding, payout, conversion, settlement, identity-sharing, verification workflows, or related connected services. This includes Banxa where Banxa is involved in a user's connected service experience.

Such sharing may include information reasonably necessary to create or administer a connected workflow, verify eligibility, support transaction or payout status, manage disputes or escalations, maintain accurate records, prevent fraud, comply with law, or otherwise support a connected service.

6.3 Compliance, Legal, and Regulatory Recipients

Baldivicio may disclose information to regulators, courts, law enforcement agencies, government bodies, tax authorities, sanctions authorities, self-regulatory bodies, auditors, legal advisors, investigators, or other competent authorities where disclosure is required, permitted, or reasonably necessary under applicable law or legal process.

This may include information associated with accounts, transactions, device and access records, compliance review materials, support records, and other information relevant to an investigation, legal obligation, or lawful request.

6.4 Corporate Transactions and Business Changes

If Baldivicio is involved in a merger, acquisition, financing, reorganization, sale of assets, insolvency proceeding, or similar corporate event, personal information may be disclosed or transferred as part of evaluating, negotiating, completing, or administering that transaction, subject to applicable confidentiality and legal requirements.

6.5 Protection of Rights, Safety, and Integrity

Baldivicio may disclose information where it reasonably believes disclosure is necessary to prevent fraud, protect users, protect the platform, respond to security incidents, investigate misconduct, enforce agreements or policies, preserve evidence, or establish, exercise, or defend legal claims.

6.6 With Your Direction or Consent

Baldivicio may disclose information where you instruct or authorize the disclosure, or where applicable law otherwise permits disclosure based on your consent.

7. Third-Party Providers, Including Banxa

Certain services connected to the Baldivicio experience may involve third-party providers such as Banxa. When such providers are involved, information may move between Baldivicio and the provider in order to support connected services, including onboarding coordination, KYC-related workflows, order-state

management, payout or conversion handling, dispute support, service troubleshooting, and legal or compliance processes.

Third-party providers may also independently collect information directly from you when you interact with them. Their handling of information may be governed by their own privacy policies, terms, notices, or legal obligations.

Baldivicio is not responsible for the independent privacy practices of third-party services except to the extent required by law. Users should review the privacy disclosures of relevant third-party providers before engaging with their services.

8. Blockchain Privacy and Public-Ledger Disclosures

Because Baldivicio supports USDC activity on Ethereum Mainnet, certain transaction-related information may exist on a public blockchain outside Baldivicio's control.

Public blockchains are not private databases. Depending on how a transaction is structured and how public blockchain data is analyzed, the following may be visible to third parties:

- wallet or address activity;
- transaction amounts;
- timestamps;
- transaction hashes;
- transfers between addresses;
- interactions with external addresses or smart contracts where relevant; and
- historical relationships between addresses over time.

Even if Baldivicio does not publicly display your identity, public blockchain data may in some circumstances be linked, inferred, or correlated to a user by Baldivicio, analytics providers, counterparties, regulators, investigators, or other third parties.

Blockchain records are generally persistent and may remain visible indefinitely, even if your Baldivicio account is later restricted, suspended, or closed. Accordingly, account closure or deletion of certain off-chain records does not remove transaction information from public blockchain infrastructure.

9. Cookies, Similar Technologies, and Technical Tools

If you visit Baldivicio's website or use in-app web content, Baldivicio and its service providers may use cookies, logs, software development kits, pixels, local storage, or similar technologies to operate services, maintain session integrity, support security, understand usage patterns, measure performance, remember user settings, and improve the service.

The exact technologies used may change over time. In some cases, your browser or device settings may allow you to limit or manage certain technologies. However, disabling some technologies may reduce functionality, impair performance, or interfere with secure use of the service.

10. Data Retention

Baldivicio may retain personal information for as long as reasonably necessary for the purposes described in this Policy, including to provide the service, comply with legal obligations, maintain business and compliance records, resolve disputes, enforce agreements, investigate misconduct, preserve evidence, protect platform integrity, and support lawful audits or inquiries.

Retention periods may vary depending on the category of information and the reason for retention. For example, Baldivicio may retain onboarding and identity-verification records, compliance records, transaction records, communications, incident logs, audit trails, device and access records, and legal or investigative materials for longer periods where required or justified by law, regulation, dispute risk, fraud prevention, or security needs.

When Baldivicio no longer needs information for the purposes described in this Policy, it may delete, de-identify, aggregate, or otherwise dispose of the information, subject to technical feasibility, legal obligations, and the persistence of public blockchain records.

11. Data Security

Baldivicio applies administrative, technical, organizational, and operational measures intended to protect personal information from unauthorized access, destruction, loss, misuse, alteration, or disclosure.

These measures may include access controls, authentication measures, environment segregation, monitoring, encryption or protected transmission where appropriate, audit logging, vendor controls, incident-response measures, data minimization where reasonably practicable, and other safeguards designed to support confidentiality, integrity, and availability.

However, no security program can eliminate all risk. Digital systems, mobile devices, communications channels, cloud environments, and blockchain-connected services all involve inherent security risks. Baldivicio therefore cannot guarantee absolute security.

Users also play an important role in protecting information by safeguarding credentials, protecting device access, using official support channels, reviewing communications carefully, and promptly reporting suspected fraud, unauthorized access, or suspicious account activity.

12. International Data Transfers

Baldivicio may process or store personal information in multiple jurisdictions depending on its operations, infrastructure, vendor arrangements, support structure, or legal obligations.

Where personal information is transferred across borders, Baldivicio may take steps designed to support lawful transfer and appropriate protection, which may include contractual safeguards, internal governance measures, vendor due diligence, or other mechanisms recognized under applicable law.

Because laws differ across jurisdictions, transferred information may in some circumstances become subject to access by regulators, courts, law enforcement, or other authorities in the jurisdiction where the information is processed or stored.

13. Your Rights and Choices

Depending on the law that applies to you, you may have rights relating to your personal information. These may include the right to request access to personal information, request correction of inaccurate information, request deletion of certain information, request restriction of processing, object to certain processing, withdraw consent where consent applies, request portability of certain data, or lodge a complaint with a competent authority.

These rights are not absolute. Baldivicio may decline, limit, or defer a request where permitted by law, including where the request would interfere with legal obligations, fraud prevention, compliance screening, dispute resolution, security measures, other users' rights, evidentiary preservation, or the integrity of the service.

Baldivicio may also need to verify your identity before acting on a rights request. In some cases, certain information may remain retained despite a request because of legal, regulatory, investigative, security,

operational, or evidentiary requirements, or because the information exists on a public blockchain outside Baldivicio's control.

Users may also update certain account information through the app or by contacting Baldivicio through the official support channel, subject to account status and verification requirements.

14. Marketing and Communications Preferences

Baldivicio may send communications necessary to operate the service, including legal notices, onboarding requests, account alerts, fraud notices, review requests, transaction-related notices, policy updates, and support messages. These communications are generally not optional where they are necessary for service delivery, compliance, or security.

If Baldivicio sends optional marketing or promotional communications, users may have the ability to opt out or adjust preferences through the app, through communication settings, or by using unsubscribe tools where provided. Even if you opt out of optional marketing messages, Baldivicio may still send non-promotional communications necessary to operate the service or comply with law.

15. Children and Minors

Baldivicio is not intended for use by children or by individuals who are not legally eligible to use the service under applicable law and Baldivicio's terms.

Baldivicio does not knowingly provide its services to users who are not legally eligible to hold an account. If Baldivicio becomes aware that personal information has been collected in connection with an ineligible user, it may take appropriate steps, including restricting the account, requesting additional information, or deleting certain off-chain information where appropriate and permitted by law.

16. Automated Review, Screening, and Decision Support

Baldivicio may use automated tools, scoring systems, rule-based systems, analytics, and other decision-support methods to help detect fraud, verify information, assess risk, screen for sanctions or other legal restrictions, review transaction activity, manage account security, and support operational decision-making.

Automated methods may contribute to decisions such as whether to request additional information, delay a transaction, escalate a case for manual review, limit functionality, or otherwise apply controls. Baldivicio may also use human review in combination with automated systems, particularly for higher-impact decisions or where further investigation is appropriate.

Depending on applicable law, you may have rights relating to certain automated processing. Baldivicio may limit or deny such requests where law permits, including where the relevant processing is necessary for fraud prevention, legal compliance, contract performance, service security, or another recognized basis.

17. Account Closure, Restriction, and Post-Closure Information Handling

If your account is restricted, suspended, frozen, reviewed, or closed, Baldivicio may continue to process and retain personal information as reasonably necessary to administer the event, complete pending obligations, preserve records, comply with law, investigate misconduct, defend claims, support audits, enforce agreements, or respond to authorities.

Closure of an account does not necessarily result in immediate deletion of related information. Some records may need to be retained for legal, regulatory, compliance, security, operational, evidentiary, or dispute-resolution reasons. In addition, transaction information recorded on public blockchain infrastructure may remain visible after closure and cannot be removed by Baldivicio.

18. Changes to This Policy

Baldivicio may update this Policy from time to time to reflect changes in law, regulation, service design, product functionality, compliance requirements, security practices, third-party arrangements, or operational needs.

If material changes are made, Baldivicio may provide notice through the mobile application, by email, on the website, or through other appropriate channels. The updated version will become effective as stated in the revised Policy or as otherwise communicated.

Your continued use of Baldivicio after an updated Policy becomes effective constitutes acknowledgment of the revised Policy, to the extent permitted by law.

19. Contacting Baldivicio About Privacy

If you have questions about this Policy, want to exercise privacy rights available to you, or need to report a privacy-related concern, you should contact Baldivicio through the official support channel made available through the mobile application or website.

When contacting Baldivicio about privacy matters, you may be asked to provide information necessary to verify your identity and locate the relevant records.

20. Final Acknowledgment

By using Baldivicio, you acknowledge and understand that:

- Baldivicio may collect and process personal information relating to identity, account activity, device and access signals, support interactions, legal compliance, and blockchain-connected services;
- Baldivicio currently supports USDC-only activity on Ethereum Mainnet through a custodial model;
- certain information relating to transactions may exist on public blockchain infrastructure and may remain visible indefinitely;
- certain connected services may involve third-party providers, including Banxa, with their own systems and privacy practices; and
- Baldivicio may process and disclose personal information where necessary to provide the service, comply with law, protect users, prevent fraud, maintain security, and preserve the integrity of the platform.

If you do not understand or accept the practices described in this Policy, you should not use Baldivicio until you obtain additional clarification.