BALDIVICIO & CO.

ISO/IEC 27562 Privacy Guidelines for Fintech Services

Document Title
Baldivicio ISO/IEC 27562 Privacy Guidelines for Fintech Services Compliance Paper

Document Type
Standards-oriented compliance and privacy governance narrative

Subject
Privacy governance, personal-information handling, transparency, financial-service data stewardship, and customer-information protection within Baldivicio

Effective Date
April 13, 2026

1. Introduction

This paper explains Baldivicio's privacy posture through the lens of ISO/IEC 27562 and its focus on privacy guidelines for fintech services. It is intended to provide a comprehensive and structured account of how Baldivicio's service model, onboarding framework, custodial account design, transaction environment, communications practices, compliance processes, support operations, and privacy controls work together to support responsible handling of personal information within a digital financial-services context.

Baldivicio is a digital financial services platform made available primarily through its mobile application. Across its service, privacy, operational, and legal materials, Baldivicio states that it currently supports USDC-only activity on Ethereum Mainnet through a custodial model, that it performs identity and compliance-related review in connection with onboarding and ongoing account use, that it may apply fraud, security, and legal controls to supported account activity, and that certain connected services may involve third-party providers such as Banxa. These characteristics are central to the privacy posture described in this paper because they establish that Baldivicio operates in a regulated, security-sensitive, blockchain-connected, and user-facing fintech environment in which personal information handling is deeply integrated into service delivery.

This paper is written as a governance and compliance document. It is not a customer marketing statement, not a substitute for legal advice, and not a technical system blueprint. Its purpose is to articulate, in standards-oriented language, how Baldivicio's service framework addresses privacy expectations that are particularly relevant to fintech services, including transparency, data minimization considerations, lawful use, rights handling, disclosure controls, retention governance, customer communications, third-party data flows, and the interaction between privacy protection and operational, legal, and financial-crime controls.

2. Purpose and Objectives

The purpose of this paper is to document how Baldivicio's privacy framework aligns with the major privacy themes raised by ISO/IEC 27562 in the context of fintech services.

Fintech services involve processing of identity information, account information, transactional information, behavioral information, security-related information, and legal or compliance-related information in environments where trust, transparency, speed, digital delivery, financial risk, and regulatory obligations must coexist. Baldivicio's service framework reflects those realities. The purpose of this paper is therefore to set out how privacy governance is embedded across Baldivicio's service model rather than treated as an isolated disclosure obligation.

The objectives of this paper are fivefold.

First, it explains the fintech context in which Baldivicio processes personal information.

Second, it establishes the categories of information that Baldivicio handles and the reasons that information is used.

Third, it explains how Baldivicio's privacy posture is shaped by account onboarding, custodial wallet operations, blockchain-connected activity, security measures, compliance review, electronic communications, customer support, and third-party service relationships.

Fourth, it provides a structured narrative of transparency, user rights, disclosure limits, retention rules, security measures, and cross-border handling in a manner suited to privacy and compliance review.

Fifth, it identifies the governance boundaries of Baldivicio's privacy posture without making claims beyond what Baldivicio's service materials support.

3. Scope

This paper applies to personal-information handling within the Baldivicio service environment, including the mobile application, website interactions where relevant, onboarding and identity verification, account administration, custodial wallet functionality, supported USDC activity on Ethereum Mainnet, customer support, legal and compliance review, electronic communications, account restrictions, suspensions, freezes, closure-related processing, and connected third-party workflows to the extent those matters involve personal information.

This paper therefore addresses privacy governance as reflected in Baldivicio's handling of identity records, contact information, account information, device and access records, transaction metadata, blockchain-related information, support interactions, compliance records, incident-related information, communications records, and information shared with or received from relevant third-party providers and lawful authorities.

It should be read consistently with Baldivicio's Privacy Policy, 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, and Account Suspension, Freezing, and Closure Policy.

4. Fintech Service Context for Privacy Governance

Baldivicio's privacy posture must be understood in light of the type of service it provides. Baldivicio is not described as a traditional chartered bank or depository institution. It is described as a digital financial services platform with a custodial model, mobile-first service delivery, identity verification requirements, transaction handling controls, compliance review processes, and blockchain-connected activity involving USDC on Ethereum Mainnet.

That service context matters because privacy in fintech is shaped not only by ordinary digital-service considerations, but also by account opening, fraud prevention, customer due diligence, account security, suspicious activity controls, sanctions-related review, transactional risk, electronic-delivery practices, public blockchain visibility, and the need to preserve records for legal and operational reasons. In Baldivicio's case, privacy governance must therefore support both customer protection and the lawful, secure, and reliable operation of a custodial financial service.

This means that Baldivicio's privacy framework is necessarily broader than a simple notice about website cookies or app preferences. It must account for how personal information is used to create accounts, verify users, review transactions, secure access, communicate legal notices, respond to fraud, cooperate with lawful authorities, retain evidence, manage disputes, and administer connected third-party service experiences.

5. Foundational Privacy Position

Baldivicio's foundational privacy position is that personal information is processed as part of a digital financial-service environment that requires transparency, lawful purpose, operational discipline, security protection, and bounded disclosure.

This position is reflected in several recurring themes across the Baldivicio framework. Personal information is collected for defined operational, legal, security, and compliance purposes. Account use is conditioned on identity and eligibility review where required. Sensitive financial-service operations are supported by monitoring, authentication, access controls, and recordkeeping. Users are given notice that public blockchain activity may create privacy constraints that differ from those in purely off-chain services. Third-party-connected services are acknowledged as distinct processing environments where separate privacy practices may also apply. Records may be retained where necessary for legal, regulatory, security, dispute-related, or evidentiary reasons.

Taken together, these themes establish a fintech-specific privacy posture in which user transparency, service integrity, and regulatory accountability are treated as mutually reinforcing rather than mutually exclusive.

6. Privacy Governance Principles Applied by Baldivicio

Within Baldivicio's service model, privacy governance is best understood through a set of principles that are consistently supported by the platform's service and policy framework.

The first principle is transparency. Baldivicio explains the categories of personal information it processes, the reasons for processing, the categories of recipients to whom information may be disclosed, the role of third-party providers, the effect of blockchain visibility, the possibility of international transfers, the existence of user rights where applicable, and the limits that may apply to those rights.

The second principle is service-linked necessity. Personal-information handling is tied to the operation of the service, including onboarding, account administration, transaction handling, security, fraud prevention, legal compliance, communications, and support.

The third principle is risk-aware proportionality. Baldivicio's privacy posture is shaped by the fact that it operates in a financial-crime-sensitive and security-sensitive environment. As a result, personal information may be used not only for convenience or account administration, but also for sanctions screening, suspicious activity review, fraud detection, dispute handling, legal preservation, and service-protection measures.

The fourth principle is controlled disclosure. Baldivicio identifies categories of recipients and lawful or service-related reasons for disclosure rather than describing personal information as freely transferable or open-ended in use.

The fifth principle is retention with purpose. Information may be retained where needed for legal, regulatory, operational, dispute-resolution, investigative, security, or evidentiary reasons, and may later be deleted, de-identified, aggregated, or otherwise disposed of where appropriate, subject to legal obligations and technical limits.

The sixth principle is security-aware protection. Personal information is governed alongside access controls, authentication measures, environment segregation, monitoring, audit logging, vendor controls, and incident-response measures.

The seventh principle is user-rights recognition. Depending on applicable law, users may have rights relating to access, correction, deletion, restriction, objection, portability, consent withdrawal, and complaints, subject to legal and operational limitations.

The eighth principle is fintech-context realism. Baldivicio expressly states that some information may exist on public blockchain infrastructure and may remain visible indefinitely, even after account restriction or closure. This is a particularly important privacy principle for a custodial digital-asset service.

7. Roles and Responsibility Allocation

Within Baldivicio's privacy framework, responsibility is allocated in a structured manner.

Baldivicio is responsible for operating the service environment in which personal information is collected, used, stored, shared, retained, and otherwise processed. This includes account onboarding, transaction-related processing, communications delivery, support handling, fraud detection, legal compliance, security measures, and the governance of relationships with service providers and connected operational partners.

Users are responsible for providing truthful, accurate, current, and complete information, maintaining the security of their credentials and devices, reviewing transactions carefully, responding to verification or support requests where necessary, and understanding that some aspects of privacy in a blockchain-connected service differ from those in conventional off-chain products.

Third-party providers may process information in support of infrastructure, analytics, identity verification, compliance screening, fraud detection, communications, record storage, support tooling, and connected service functions such as those involving Banxa. Where those providers are involved, Baldivicio's privacy posture makes clear that some information may move between Baldivicio and the provider for defined service or compliance purposes, and that the provider may also have its own privacy obligations and notices.

This responsibility structure is particularly important for a fintech privacy framework because it recognizes that privacy outcomes are shaped not only by Baldivicio's direct actions, but also by user behavior, public blockchain characteristics, and connected service relationships.

8. Categories of Personal Information

Baldivicio's privacy framework supports a broad but structured view of the categories of personal information relevant to the service.

Identity and account-opening information includes data such as name, date of birth, residential address, email address, phone number, nationality, government-issued identification details, and related identity-verification materials. Depending on the context, additional information may include source-of-funds information, source-of-wealth information, occupation or employment information, expected account activity information, and declarations relevant to compliance review.

Account and profile information includes account identifiers, authentication events, account status history, communication preferences, feature usage, statement requests, proof-of-account requests, closure requests, and records relating to restriction, review, suspension, or closure.

Transaction and wallet-related information includes source and destination addresses, wallet-related records, transaction instructions, transaction hashes, timestamps, amounts, blockchain confirmations, status information, inbound and outbound transfer data, and operational notes relating to review or disposition of transactions.

Blockchain and public-ledger information may include publicly observable address relationships, transaction histories, transfers into or out of relevant addresses, exposure to higher-risk destinations, and other on-chain information relevant to compliance, security, operations, or fraud review.

Device, access, session, and technical information may include device identifiers, application version, operating system information, browser or in-app webview information where relevant, IP address, approximate location inferred from technical signals, login timestamps, session records, access history, crash or error data, performance telemetry, and network information.

Support, dispute, and communications information may include messages, attachments, complaint details, escalation records, support outcomes, communications history, dispute materials, and records of notices or messages delivered through the service.

Information from third parties may include verification results, order status, payout or settlement status, exception codes, escalation signals, fraud indicators, sanctions-screening results, public records, legal notices, or information received from service providers, regulators, investigators, or other lawful sources.

This breadth is consistent with the operational realities of a fintech service that combines account creation, custodial functionality, transaction handling, security monitoring, customer support, and legal compliance.

9. Sources of Personal Information

Baldivicio may obtain personal information from several sources, and the distinction between those sources is important for privacy governance.

Some information is provided directly by the user during onboarding, account use, customer support, dispute handling, account recovery, or closure-related interactions.

Some information is collected automatically through access to the service, including device, session, technical, and behavioral information relevant to secure and reliable service operation.

Some information arises from transaction handling and blockchain-connected activity, including on-chain data and operational metadata associated with transaction processing.

Some information is obtained from service providers and connected operational partners, including those supporting verification, communications, analytics, monitoring, customer support, fraud prevention, infrastructure, and connected financial-service workflows.

Some information may also come from public, legal, and regulatory sources, including sanctions and watchlist databases, courts, authorities, public blockchain records, fraud intelligence, and other lawful sources relevant to service integrity and compliance.

This multi-source model is particularly characteristic of fintech privacy environments, where a service must reconcile self-reported information, public information, operational information, and provider-supplied information in order to function responsibly.

10. Purposes of Processing

Baldivicio's privacy framework presents personal-information handling as purpose-driven rather than open-ended.

Personal information may be processed to provide and operate the service, including creation and administration of accounts, delivery of the mobile application and related features, maintenance of custodial wallet functionality, display of supported balances, transaction handling, account lifecycle management, customer support, statements, records, and service communications.

It may also be processed to verify identity, assess eligibility, determine whether an account may be opened or maintained, request additional documentation, support ongoing review, and confirm account ownership.

A substantial part of the processing model relates to legal, regulatory, and financial-crime obligations. This includes sanctions screening, politically exposed person screening, fraud detection, suspicious activity review, recordkeeping, lawful disclosure, internal investigations, and cooperation with competent authorities where required or permitted by law.

Personal information may also be processed to protect users, protect the platform, secure accounts, investigate unauthorized access, analyze suspicious behavior, manage risk, detect scams, prevent cyber threats, preserve evidence, respond to disputes, improve operational resilience, and maintain service integrity.

These uses are highly consistent with a privacy model designed for fintech services, where the lawful and secure operation of the service requires more than ordinary user-profile administration.

11. Transparency and User Notice

One of the most important features of Baldivicio's privacy posture is that user-facing notice is built into the service framework rather than treated as a hidden or incidental matter.

Baldivicio's Privacy Policy describes the scope of the policy, the service context, the categories of information processed, the sources of information, the uses of information, lawful bases where applicable, sharing practices, third-party service relationships, blockchain privacy constraints, cookies and similar

technologies, retention, security measures, international transfers, user rights, marketing preferences, children and minors, automated review, account-closure handling, policy changes, and contact pathways.

Additional privacy-relevant notice appears across the wider documentation set. The Customer Identification Program Notice explains why identity-related information may be collected and reviewed. The E-Sign Agreement explains how records and notices may be delivered electronically. The Account Suspension, Freezing, and Closure Policy explains that information may continue to be processed during restriction, review, or closure events. The Irreversible Transactions Disclosure explains that blockchain-based activity may become irreversible, which in turn informs user expectations about public-ledger persistence. The Terms of Service describe how privacy interacts with service delivery, account responsibilities, and third-party-connected services.

This layered notice model is a strong privacy-governance feature because it recognizes that meaningful fintech privacy transparency is often distributed across the service framework rather than contained in a single clause.

12. Legal Bases and Fintech Privacy Legitimacy

Baldivicio's Privacy Policy recognizes that different processing activities may rest on different legal bases depending on the nature of the information, the context of collection, and the law that applies.

These bases may include the need to provide the service requested by the user, the need to comply with legal or regulatory obligations, Baldivicio's legitimate interests in service integrity, fraud prevention, compliance, dispute handling, and security, the protection of important interests, and consent where consent is required or appropriate.

This is significant in a fintech privacy setting because personal-information processing often serves multiple purposes simultaneously. Identity verification may support both contract performance and legal compliance. Transaction monitoring may support both service operation and fraud prevention. Communications may be necessary both for customer service and for legal notice. Baldivicio's privacy framework accounts for this complexity without collapsing all processing into a single, oversimplified justification.

13. Identity Verification, Due Diligence, and Privacy

In a fintech environment, identity verification is one of the most privacy-sensitive activities because it involves collection of core identity records and may affect whether a person can access a service.

Baldivicio's Customer Identification Program Notice explains that identity verification may be required before or during use of the service. It states that Baldivicio may request personal identification information, government-issued identification, compliance-related information, and additional supporting materials where necessary. It also explains that Baldivicio may use automated systems, manual review, and third-party support in the verification process and may conduct ongoing or repeat review as required by risk, security, or legal developments.

From a privacy-guidelines standpoint, the importance of this framework is that the service expressly connects sensitive identity-data processing to clear purposes: verifying identity, assessing eligibility, supporting lawful onboarding, maintaining service integrity, and preventing fraud or unlawful use. The framework also communicates the consequences of non-completion or inability to verify, thereby supporting procedural transparency.

14. Transaction Privacy and Fintech Data Handling

Baldivicio's transaction environment creates a distinctive privacy posture because it combines customer account controls with blockchain-connected activity.

On the one hand, transaction handling involves ordinary fintech records such as account status, transaction instructions, service routing, timing, review notes, and support or dispute records. On the other hand, it also involves public-ledger elements such as addresses, hashes, timestamps, and transfer visibility on Ethereum Mainnet.

Baldivicio's Privacy Policy explains that it may process transaction and wallet-activity information as well as publicly observable blockchain information for compliance, security, operations, dispute review, and fraud detection. It also explains that public blockchain information may remain visible indefinitely and may be correlated or analyzed by third parties.

This dual nature of transaction privacy is one of the clearest fintech-specific privacy features in the Baldivicio framework. It demonstrates that Baldivicio does not present blockchain-linked financial activity as though it were fully private or fully erasable.

15. Public Blockchain Privacy Constraints

A privacy framework for a fintech service that interacts with public blockchain infrastructure must explicitly account for the fact that some information is not exclusively within the operator's control. Baldivicio does so in direct terms.

The Privacy Policy states that public blockchains are not private databases and that transaction-related information may be visible to third parties. It identifies address activity, transaction amounts, timestamps, hashes, transfers between addresses, interactions with external addresses or smart contracts where relevant, and historical relationships between addresses over time as forms of publicly observable information. It further explains that blockchain records may persist indefinitely and that closure or deletion of certain off-chain records does not remove those on-chain records.

This is a highly significant privacy-governance point. It helps establish realistic user expectations and recognizes a central privacy challenge for digital-asset fintech services: some transaction-related data is necessarily governed by public-ledger architecture rather than by the service operator alone.

16. Sharing and Disclosure Governance

Baldivicio's privacy posture treats sharing and disclosure as bounded activities tied to identified categories of recipients and identified purposes.

Information may be shared with service providers performing functions on Baldivicio's behalf, including cloud hosting, infrastructure support, analytics, identity verification, sanctions screening, fraud detection, compliance support, customer support tooling, record storage, security monitoring, and incident management.

Information may also be shared with third-party financial or operational partners that support connected services such as funding, payout, conversion, settlement, verification workflows, card-related functionality where applicable, dispute support, or related operational needs.

Disclosure may also occur to regulators, courts, law enforcement agencies, tax authorities, sanctions authorities, legal advisors, auditors, investigators, or other competent authorities where disclosure is required, permitted, or reasonably necessary under applicable law or legal process.

Additional disclosure may occur in connection with corporate transactions, protection of rights and safety, prevention of fraud, preservation of evidence, or user-directed or consent-based disclosures.

This approach is consistent with fintech privacy guidelines because it avoids portraying personal-information sharing as uncontrolled while still recognizing the operational and legal realities of a regulated financial service.

17. Third-Party Providers and Banxa-Connected Flows

A distinctive feature of Baldivicio's privacy framework is its express treatment of connected third-party services, especially those involving Banxa.

Baldivicio states that certain connected services may involve information flows between Baldivicio and third-party providers in order to support onboarding coordination, KYC-related workflows, order-state management, payout or conversion handling, dispute support, troubleshooting, and legal or compliance processes. At the same time, it states that such providers may independently collect information directly from the user and may operate under their own privacy policies, terms, notices, or legal obligations.

This is important because privacy in fintech often extends beyond the primary service provider. By clearly recognizing organizational boundaries and third-party privacy practices, Baldivicio supports a more accurate and transparent privacy position for users who engage with connected services.

18. Customer Support, Complaints, and Dispute Records

Fintech privacy is not limited to onboarding and transactions. It also includes support interactions, complaints, disputes, escalations, account recovery, and closure-related communications.

Baldivicio's Privacy Policy makes clear that support interactions may generate messages, attachments, account references, complaint details, escalation records, support outcomes, dispute materials, and related service notes. Communications delivered to the user, including in-app notices, emails, prompts, and support follow-up messages, may also be retained.

This is relevant to privacy-guidelines analysis because support and dispute channels often involve highly sensitive contextual information, including transaction explanations, identity-confirmation discussions, allegations of fraud, recovery requests, and account-status consequences. Baldivicio's framework recognizes these records as part of the protected and retained information environment.

19. Automated Review, Screening, and Decision Support

Baldivicio states that it 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.

The service materials also explain that 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 apply other controls, and that human review may also be used, particularly for higher-impact decisions or where further investigation is appropriate.

From a privacy-guidelines perspective, this is a significant governance point. It shows that Baldivicio does not ignore the privacy implications of automated processing. Instead, it expressly acknowledges that automated methods may be used, that such methods may affect service outcomes, and that users may have rights relating to some automated processing depending on applicable law.

20. User Rights and Procedural Fairness

Baldivicio states that, depending on applicable law, users may have rights relating to access, correction, deletion, restriction, objection, portability, consent withdrawal, or complaint submission. It also explains that these rights are not absolute and may be limited where necessary to comply with law, preserve evidence, maintain fraud prevention, support compliance screening, protect the rights of others, or preserve the integrity of the service.

This is a particularly important part of a fintech privacy framework. In financial services, privacy rights often interact with non-waivable obligations concerning recordkeeping, fraud prevention, suspicious activity review, sanctions obligations, dispute handling, and legal preservation. Baldivicio's approach is to recognize user rights while openly stating that those rights may operate within legal and operational boundaries.

That balance between rights recognition and lawful limitation is consistent with a pragmatic privacy-guidelines posture for a fintech service.

21. Retention, Deletion, and Evidentiary Preservation

Baldivicio's Privacy Policy provides a detailed retention framework. Personal information may be retained as long as reasonably necessary 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.

The policy further states that retention periods may vary by category of information and by reason for retention. Examples include onboarding and identity-verification records, compliance records, transaction records, communications, incident logs, audit trails, device and access records, and legal or investigative materials. When information is no longer needed, Baldivicio may delete, de-identify, aggregate, or otherwise dispose of it, subject to technical feasibility, legal obligations, and the persistence of public blockchain records.

This is particularly well aligned with a fintech privacy-guidelines approach because it acknowledges both the necessity of retention and the importance of eventual disposition where appropriate.

22. Information Security and Protection Measures

Privacy governance in fintech depends heavily on information security. Baldivicio's Privacy Policy states that the platform applies administrative, technical, organizational, and operational measures intended to protect personal information from unauthorized access, destruction, loss, misuse, alteration, or disclosure.

The examples given include access controls, authentication measures, environment segregation, monitoring, encryption or protected transmission where appropriate, audit logging, vendor controls, incident-response measures, and data minimization where reasonably practicable. Users are also assigned a role in protecting information by safeguarding credentials, protecting device access, using official support channels, and promptly reporting suspected fraud or suspicious activity.

This protection model is relevant to ISO/IEC 27562 because privacy in fintech depends not only on policy statements but also on the security measures that preserve confidentiality, integrity, and availability of personal information.

23. International Transfers and Multi-Jurisdictional Privacy Handling

Baldivicio states that personal information may be processed or stored in multiple jurisdictions depending on operations, infrastructure, vendor arrangements, support structure, or legal obligations. It also states

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

This is a material privacy-governance issue for a fintech service because digital financial operations often involve globally distributed infrastructure, cloud services, support arrangements, and compliance relationships. Baldivicio's framework recognizes that cross-border handling requires governance rather than being treated as an invisible background detail.

24. Electronic Communications and Privacy

Baldivicio's E-Sign Consent and Electronic Communications Agreement is also an important part of the privacy framework. It explains the categories of communications that may be delivered electronically, the methods by which such communications may be delivered, the user's responsibility to keep contact information current, the possibility of requesting paper copies, the consequences of withdrawing consent, and the fact that many service communications are delivered through the app or related electronic channels.

From a fintech privacy-guidelines standpoint, this matters because communications often contain personal information, legal information, account information, or security-related information. A privacy-aware electronic-communications model therefore contributes to the overall protection and transparency of the service.

25. Marketing, Preferences, and Optional Communications

Baldivicio distinguishes between communications necessary to operate the service and optional marketing or promotional communications. The Privacy Policy states that service-related communications, including legal notices, onboarding requests, fraud notices, account alerts, and support messages, are generally not optional where necessary for service delivery, compliance, or security. Optional marketing communications, where offered, may be subject to opt-out or preference controls.

This distinction is an important privacy-governance feature because it separates essential fintech communications from optional engagement communications and helps users understand which messages are functionally necessary to maintain safe and lawful service delivery.

26. Children, Eligibility, and Sensitive Service Access

Baldivicio states that it 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. It further states that if it becomes aware that personal information has been collected in connection with an ineligible user, it may take appropriate steps, including restriction of the account, requests for additional information, or deletion of certain off-chain information where appropriate and permitted by law.

This is a relevant privacy-governance point because fintech services often involve heightened sensitivity around eligibility, age, and lawful access. Baldivicio's framework treats this as a matter of both privacy and service integrity.

27. Account Restriction, Suspension, Closure, and Post-Closure Privacy Handling

Baldivicio's privacy posture extends beyond the active life of an account. The Privacy Policy states that if an 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.

This is reinforced by the Account Suspension, Freezing, and Closure Policy, which explains that closure does not necessarily eliminate legal, compliance, recordkeeping, or investigative obligations. It is also reinforced by the blockchain privacy disclosures, which explain that on-chain transaction records may remain visible after closure and cannot be removed by Baldivicio.

This is a strong example of a fintech-appropriate privacy rule: privacy obligations continue through and beyond operational closure events, and deletion is not assumed to be immediate or absolute.

28. Relationship Between Privacy, Compliance, and Financial-Crime Controls

One of the most important features of a fintech privacy framework is its ability to coexist with compliance and financial-crime controls. Baldivicio's framework demonstrates this clearly.

Privacy is not described as a barrier to lawful screening, onboarding review, fraud prevention, suspicious activity response, sanctions compliance, or cooperation with authorities. At the same time, those controls are not presented as reasons to dispense with transparency altogether. Instead, Baldivicio explains why information is collected, how it may be used, what kinds of controls may be applied, when information may be disclosed, and how rights may operate within those constraints.

This integrated posture is particularly well suited to privacy guidelines for fintech services because it reflects the practical reality that privacy, trust, safety, compliance, and operational integrity must work together in financial technology environments.

29. Conformance-Oriented Reading of ISO/IEC 27562 Themes

Read against the broad themes associated with privacy guidelines for fintech services, Baldivicio's service framework supports a coherent privacy narrative.

It supports transparency by explaining categories of personal information, sources of information, purposes of processing, sharing practices, retention, rights, international transfers, and blockchain-specific privacy limits.

It supports purpose-linked processing by tying information handling to account administration, identity verification, transaction handling, fraud prevention, security, legal compliance, support, communications, and service improvement.

It supports bounded disclosure by identifying categories of recipients and lawful or service-related reasons for disclosure.

It supports user awareness of third-party data flows by addressing Banxa-connected services and other provider relationships.

It supports fintech-specific privacy realism by expressly addressing public blockchain visibility and the persistence of on-chain records.

It supports security and integrity by identifying access controls, authentication measures, monitoring, protected transmission where appropriate, vendor controls, audit logging, and incident-response measures.

It supports rights handling by recognizing access, correction, deletion, objection, portability, restriction, consent withdrawal, and complaint rights where applicable, while also recognizing lawful limits.

It supports retention and post-closure governance by describing legal, operational, investigative, and evidentiary reasons for retaining information and by acknowledging that some information may remain visible or retained after account closure.

It supports automated-processing transparency by explaining that automated review and scoring may be used in support of fraud prevention, legal screening, and account security.

Taken together, these themes support a standards-oriented reading of Baldivicio as a fintech service with a defined and layered privacy governance framework.

30. Boundaries of This Paper

This paper is intentionally limited to matters established by Baldivicio's service descriptions, privacy framework, and related policies and disclosures.

It does not describe technical implementation details that are not stated in those materials. It does not specify underlying database architecture, deployment topology, proprietary fraud models, internal case-management tools, encryption configurations, infrastructure segmentation maps, or any other technical feature not expressly described in Baldivicio's service framework.

It also does not convert legal disclosures into promises beyond what they say. Where Baldivicio's materials describe a privacy objective, governance principle, or operational authority at a high level, this paper states that matter at the same level and does not transform it into an unsupported technical or regulatory claim.

31. Conclusion

Baldivicio's service framework establishes a clear privacy posture for a fintech environment. The platform is delivered digitally, depends on identity verification and account controls, processes sensitive user and transaction-related information, interacts with public blockchain infrastructure, relies in part on third-party providers, and operates in a security-sensitive and compliance-sensitive context.

The resulting privacy environment is not limited to a general consumer-data notice. It is a structured governance framework that addresses collection, use, disclosure, electronic communications, support interactions, international transfers, automated review, financial-crime controls, public-ledger visibility, retention, post-closure handling, and user rights in a coordinated way.

Accordingly, Baldivicio's ISO/IEC 27562 privacy posture is best characterized as a fintech-specific, transparency-oriented, control-driven privacy framework in which personal information is handled through defined service purposes, lawful governance measures, user-facing disclosures, operational security protections, and bounded sharing and retention practices.

32. Final Statement

This paper should be read as Baldivicio's ISO/IEC 27562 privacy-guidelines compliance narrative in the context of its digital financial-services model. It reflects the privacy practices, service design, operational safeguards, and governance principles expressed across Baldivicio's published policies, disclosures, and service descriptions, and it should be interpreted consistently with those materials.