PRIVACY POLICY

Last updated: June 2025

This Privacy Policy explains how **Consultora Blockchain S.R.L.**, headquartered in the city of La Paz, Bolivia, in its role as **Data Controller**, collects, uses, protects, and retains the personal data of users who use the **Wira Wallet**application.

Wira Wallet is designed to operate in a fully **non-custodial** manner. All private keys, credentials, and documents are generated, encrypted, and stored directly on the user's device. Neither Consultora Blockchain nor third parties have technical access to these data after installation.

This policy is issued in compliance with current Bolivian legislation, including:

- **Law No. 1082** on Digital Citizenship
- **Law No. 164** on Telecommunications and Information and Communication Technologies
- **Supreme Decree No. 3525** on Digital Signature

1. Personal Data Collected

Wira Wallet collects only the information strictly necessary to create your **sovereign digital identity** and allow you to use the **non-custodial wallet**:

- **National ID (DNI)** — number and front/back photos: captured with the camera, processed by a local OCR, and verified through Polygon ID; the encrypted file (**AES-256-GCM**) remains in the device's Keystore.
- **Selfie**: captured with the camera; the 1-to-1 biometric comparison is performed on the device; the image remains encrypted, and we do not store this information.
- **Decentralized Identifier (DID)**: generated on the phone and signed with the local key; only its hash is published on the blockchain.
- **Sovereign Credential (VC)**: issued with Polygon ID after validating DNI + selfie; encrypted with a key derived from your PIN (**Argon2**) and stored in **Ceramic**. Its validity is demonstrated through **zero-knowledge proofs (zk-SNARK)**, meaning anyone can verify authenticity without seeing your data.
- **On-chain addresses and transaction hashes**: created when you sign operations; public by nature but do not contain personal information.

Important: Consultora Blockchain cannot decrypt user credentials or access documents, as they remain encrypted locally or are validated through proofs that do not reveal content.

2. Purposes of Processing

Personal data are used exclusively for the following purposes:

- Verify the user's identity (DNI + selfie) and issue their sovereign credential (VC).
- Enable and operate a non-custodial wallet via **Account Abstraction**.
- Allow local sign-in using **PIN** or **biometrics**.
- Implement **on-chain recovery** using **guardians**.
- Collect anonymous technical metrics to improve the App's security and stability.

3. Legal Basis

Data processing is based on:

- The user's **express consent** (Art. 21 of the Political Constitution of the State and Law No. 1082).
- **Performance of a digital contract** for the use of the application (Art. 78 of Law No. 164).
- **Advanced electronic signature**, pursuant to Supreme Decree No. 3525, to authorize **on-chain** transactions.

4. Data Recipients

Personal data will not be sold, transferred, or shared with unauthorized third parties. The only exceptions include:

- **Decentralized technical providers** (such as Ceramic nodes or RPC services), used exclusively to operate the network.
- **Judicial or administrative authorities**, only upon a duly issued legal request and subject to user-governance authorization. Otherwise, it is not technically possible to decrypt the user's data.

5. Data Storage and Retention

- All sensitive data are encrypted locally using robust algorithms (**AES-256-GCM**).
- Credentials are stored encrypted in the **Ceramic** network, and their validity is demonstrated with **zero-knowledge proofs**.
- Data deletion must be performed by the user through in-app functions that are recorded in the application's **smart contracts**.

6. User Rights

The user may exercise the following rights at any time:

- **Access** to their encrypted personal data.
- **Rectification** of errors identified in issuance processes.
- **Portability** of their credentials between devices.

These rights can be exercised only through the functions enabled within the application.

7. Information Security

We implement multiple layers of security:

- **End-to-end encryption** of all sensitive data.
- **Local storage** of sensitive data (**Android Keystore**).
- **Smart contracts** and **zero-knowledge proofs** to protect identity.
- **Strengthened authentication** via PIN and biometrics.

8. Changes

This Policy may be updated to reflect regulatory or technological changes. We will notify such changes through the application and update the date at the beginning of this document.