LocalWallet Global Privacy Policy

I. Introduction

This Global Privacy Policy (the “Policy”) describes how we process data in connection with the use of the LocalWallet mobile application (the “Application”) and the related website available at localwallet.com (the “Website”). By using the Application or the Website, you accept the rules described in this Policy, so please read it carefully.

LocalWallet is a non-custodial crypto-asset wallet. This means that sole control over the private keys and the funds rests with the user, and we at no stage obtain access to the user's private keys, recovery phrase (seed phrase) or funds. As a result, the scope of data that reaches us at all is, by design, very limited.

Data controller. The data controller is Decentechnology Inc., a company formed in the Union of the Comoros under The International Business Companies Act 2014, registration number HT00126005, with its registered office at: Bonovo Road, Fomboni, Island of Mohéli, Union of the Comoros (the “Controller”, “we” or the “Company”).

Contact. For all matters relating to personal data, including in order to exercise your rights, you can contact us at the e-mail address: **support@localwallet.com**.

Definitions. For the purposes of the Policy, the following meanings apply:

- “Personal data” means any information relating to an identified or identifiable natural person, in particular an online identifier, location data or other factors determining identity.
- “Processing” means any operation performed on personal data, such as collection, recording, storage, use, disclosure, erasure or destruction.
- “Cookies” means small text files stored on the device through which the user accesses the Website.

Principles. We process personal data lawfully, fairly and transparently; we collect it for specified and legitimate purposes; we limit it to what is necessary; we keep it accurate; we store it no longer than necessary; and we ensure its appropriate security through technical and organisational measures.

We may update the Policy; continued use of the Application or the Website after changes have been introduced means that you have reviewed its current version.

II. Territorial scope and applicable law (EEA and outside the EEA)

The Policy is global in nature and applies to all users, regardless of where the Application or the Website is used.

For users accessing the Application or the Website from the territory of the European Economic Area (EEA), Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) applies. The provisions marked in the Policy as relating to users from the EEA (legal bases for processing, data subject rights, rules on transfers outside the EEA, and the right to lodge a complaint) apply to those users.

For users accessing the Application or the Website from outside the EEA, processing takes place in accordance with this Policy and the applicable local law. Such users may have analogous rights under their local law; in any matter they can contact us at the address indicated in section I.

III. The key principle: we do not have access to your keys or funds

LocalWallet is non-custodial. In particular:

- The private keys and the recovery phrase (seed phrase) are generated and stored exclusively on your device. They are never transmitted to us or stored by us.
- We do not have access to your funds and cannot dispose of them. Every transaction requires your signature in the Application.
- We cannot block, seize or recover your funds. If you lose the recovery phrase, we are unable to restore access to the wallet.
- You can at any time import your recovery phrase into another wallet and use the funds independently of us.

No KYC procedures. We do not verify users' identity. We do not require or collect identity documents, biometric data, bank account data or similar identification data.

IV. What data we process, for what purpose and on what basis

The table below sets out the categories of data processed, the purposes of processing and the legal bases (GDPR) applicable to users from the EEA.

Category of data	Purpose of processing	Legal basis (users from the EEA)
Public wallet address	Identifying the user at the server layer, authentication by means of a signature, providing the functions of the Application	Article 6(1)(b) GDPR (performance of a contract) and (f) (legitimate interest: operation and security of the service)
Technical data and logs (IP address, device type and version, operating system and Application version, timestamps)	Security, abuse prevention, error diagnostics, infrastructure maintenance	Article 6(1)(f) GDPR (legitimate interest)
Crash data and analytics data (where such tools are used)	Improving the stability and quality of the Application	Article 6(1)(a) GDPR (consent) or (f) (legitimate interest), depending on the configuration
One-time pairing and matching codes (exchange function, pairing with the Kanga service)	Technically enabling two exchange parties to be connected or a wallet to be paired; the codes are one-time and contain no user-identifying data	Article 6(1)(b) and (f) GDPR
Data provided in correspondence (e.g. e-mail address and the content of a support request)	Handling enquiries and requests, archiving correspondence	Article 6(1)(b) and (f) GDPR
Push notification token (if you enable notifications)	Sending notifications for which consent has been given	Article 6(1)(a) GDPR (consent)

We do not collect data that is not necessary for the operation of the service. Providing data is voluntary; however, the absence of certain data (e.g. the wallet address) may make it impossible to use the Application.

V. Data recipients and processors

Data may be entrusted to trusted providers acting on our behalf, in particular providers of infrastructure and hosting, providers of analytics and crash-reporting tools, providers of push-notification services, and providers of blockchain access infrastructure (nodes, RPC services). With entities processing data on our behalf we conclude data processing agreements compliant with the requirements of applicable law (with respect to users from the EEA, Article 28 GDPR).

Data may be disclosed to competent authorities or other authorised entities where required by applicable law, to the extent that we hold such data.

VI. Transfers of data outside the European Economic Area (EEA)

The Controller is established in the Union of the Comoros, and some providers may process data outside the EEA. Use of the Application or the Website therefore involves the transfer of data outside the EEA. The Union of the Comoros is not covered by a European Commission adequacy decision.

With respect to users from the EEA, where data is transferred outside the EEA we apply the safeguards required by the GDPR, in particular the standard contractual clauses (Article 46 GDPR) or other appropriate bases provided for in Chapter V of the GDPR. You can obtain a copy of the safeguards applied by contacting us at the address indicated in section I.

VII. No profiling or automated decision-making

We do not take decisions in relation to users based solely on automated processing, including profiling, that produce legal effects concerning them or similarly significantly affect them, within the meaning of Article 22 GDPR. Where we use tools that automatically analyse data (e.g. statistics, diagnostics), this does not produce such effects.

VIII. Your rights

With respect to users from the EEA, in connection with the processing of data you have the right to:

- access to the data and to obtain information about the processing,
- rectification of inaccurate or incomplete data,
- erasure of the data,
- restriction of processing,
- object to processing based on legitimate interest,
- data portability,
- withdraw consent at any time, without affecting the lawfulness of processing carried out before the withdrawal,
- lodge a complaint with the competent supervisory authority. If you are a user from the EEA, the competent authority is the supervisory authority of your country of habitual residence, place of work or place of the alleged infringement.

Due to the non-custodial nature of the service and the characteristics of blockchain technology, the exercise of certain rights may be limited. Transactions recorded on a public blockchain are public, permanent and immutable; we do not control that network and cannot change, hide or delete data already recorded in it, and therefore the exercise of, for example, the right to erasure with respect to such data may be technically impossible.

Users outside the EEA may have analogous rights under the applicable local law. To exercise your rights, contact us at the address indicated in section I.

IX. Retention period

We retain data only for as long as necessary to achieve the purposes set out in section IV, after which we delete or anonymise it. Technical data and logs are usually retained for up to 12 months. Correspondence is retained for the period necessary to handle the matter and for the possible establishment, exercise or defence of claims. Data processed on the basis of consent is retained until the consent is withdrawn.

X. Security

We apply appropriate technical and organisational measures to protect data against unauthorised access, loss or alteration. Please note, however, that the security of your funds depends primarily on the secure storage of the recovery phrase, to which we have no access and which we are unable to reconstruct.

XI. Cookies (Website)

The Application itself is a non-custodial wallet and stores the data necessary for its operation locally on the user's device. The following rules apply to the Website.

The following types of cookies and similar technologies may be used on the Website:

- necessary, required for the proper functioning of the Website,
- analytics and statistics, used to analyse traffic and improve the Website, applied with the user's consent,
- marketing, used to present content tailored to the user, applied with the user's consent.

Necessary cookies do not require consent. We use analytics and marketing cookies only with the consent expressed by the user, which can be withdrawn or changed at any time in the settings of the Website or the browser. Most browsers accept cookies by default; the user can restrict or disable this in the browser settings, which may affect the functioning of the Website.