DATA PRIVACY MANIFESTO

PREAMBLE

This manifesto will provide the guidelines for the technology development of the MOBIX Ecosystem. These guidelines will ensure that MOBIX technology follows our highest standards on data privacy including compliance with privacy frameworks like GDPR and CCPA. We however go further and stretch beyond the letter of the law on these matters.

Privacy, as defined by the Cambridge Dictionary, is the right to keep personal matters and relationships secret. MOBIX provides its users with full control over their data and enables them to keep full control over their data. However, users can freely choose to monetize their data, by earning MOBIX Miles & MOBX Tokens.

This monetization will not suffer from the tradeoffs between ease of use and privacy due to our "Privacy by Design" approach to building technology. The goal with this design philosophy is to build technology and processes that "Cannot be Evil " as opposed to merely stating that we adhere to a motto like the famous "Don't be Evil" of the early days of Google.

Privacy by Design Principles

- Proactive not reactive; preventive not remedial:
    - This means that in our design process, we're thinking ahead and preventing the accumulation of data which could be abused as opposed to attempting to defend against and remediate data leaks.
- Privacy as the default:
    - This means that by design you don't have to do anything extra to get the highest level of privacy with MOBIX. You won't be confronted with a complex "privacy dashboard" or need to get a PHD in data science to decide whether it's safe to use MOBIX products.
- Privacy embedded into design:
    - This means that within MOBIX, privacy isn't an afterthought or an add on or something buried in the settings or terms and conditions. It also means that we will design our MOBIX processes such that the correlation of real world user identities with their pseudo anonymous identifiers / addresses is impossible. We won't track you and we won't build tech that enables others to do so.
- Full functionality – positive-sum, not zero-sum
    - We fundamentally reject false tradeoffs and dichotomies such as "privacy versus security" and MOBIX products demonstrate that it is possible to have highly usable data driven applications without sacrificing privacy or user sovereignty.
- End-to-end security – full lifecycle protection
    - In simple terms this means that where user associated data does accumulate, processes are designed to keep that data secure and to delete it as soon as it has served its primary purpose. It means that we won't "incidentally" be building data lakes and correlating or identifying users for targeting.
- Visibility and transparency – keep it open
    - This means that we are transparent about where data is accumulated, how it is handled and when it will be deleted whenever the data in question isn't fully in the sovereign control of MOBIX users. In the future we plan to offer individual users privacy preserving autonomous economic agents that can proactively manage privacy, and ensure visibility throughout the data lifecycle.
- Respect for user privacy – keep it user-centric
    - This means that we promise to not go off the rails on privacy and to prevent mission creep. We're committed to maintaining the highest level of data protection for users and will remain so.

MOBIX Practical Data Protection and Privacy Principles

1. MOBIX collects only enough data to fulfil our transparently stated narrow purposes
2. Where possible, MOBIX anonymizes data.
    a. Where anonymization and de-identification of data are not fit for purpose, MOBIX pseudonymises data.
    b. MOBIX never uses personal identifiable information without robust encryption.
    c. MOBIX only uses encrypted personal identifiable information as a last resort when all other levels of anonymization, de-identification and pseudonymization have proven not fit for our transparently stated narrow purposes.
    d. MOBIX always employs a time-limited data lifecycle. Once the transparently stated narrow purposes for which data has been accumulated are complete, data will be deleted within a reasonable time frame. MOBIX will not build or operate data lakes of personal information.
3. MOBIX ensures complete pseudonymization and/or anonymization of personally identifiable information on edge devices, e.g. smartphone, before transmitting it across network connections.
4. MOBIX commits to open-sourcing the security and privacy relevant business logic of the system for public inspection.
5. MOBIX employs an AI and data science ethics checklist directly in the codebase.
6. MOBIX adheres to GDPR regulations and adheres to the Ethics Guidelines For Trustworthy Ai set forth by the European Commission.

MOBIX Wallet Data

The MOBIX Wallet is the first application in the MOBIX ecosystem, which focuses on use cases in the micromobility industry. Different data assets are produced by using the MOBIX Wallet applications as well as third party services. The following data assets will be described by data type, data custody and access, potential value and utility, as well as identifiers used.

1. Location and Movement Data

When starting a trip with the MOBIX wallet, location and movement data is created. In order to optimise the trip detection, MOBIX may over short terms transmit the following data from the app for analysis: Speed, altitude, location (GPS).

Proof that your movement pattern matches the typical micromobility pattern is created directly on your device, this proof is sent to the MOBIX Reward AEA to reward you with MOBIX Miles. The pseudonymous identifier used is your MOBIX address, which is needed to credit you MOBIX Miles.

2. MOBIX Miles Data

The MOBIX wallets offer you tasks, like “Refer a Friend” or “Trips”, to earn MOBIX Miles. The amount of MOBIX Miles, the tasks and the time you earned it is available for you and the MOBIX

team. This allows us to see how effective our MOBIX challenges are. As an identifier, we use your pseudonymous MOBIX address, which is needed to credit you MOBIX Miles and MOBX tokens.

3. App Usage Data

How you use our app, the patterns of your clicks, screen time and how often you open the app per day gives MOBIX team valuable insights and allows us to create a smooth user experience for you. This data is only available for the MOBIX team and will not be shared or sold to target you. It will also not be used to correlate or deanonymize users or map the pseudonymous MOBIX address to public user identities such as social media accounts.

4. Wallet Behaviour

Transactions on the Fetch.ai blockchain are all public and can be inspected on their block explorer. Therefore, any transaction, like incoming and outgoing transfers, e.g. through the Reward AEA or Smart Contract interactions, e.g. staking, are public to everyone. Also here, your MOBIX address is used as a pseudonymous identifier.

5. Agentverse (Fetch.ai)

To offer you Agentic AI features in the MOBIX app, such as automatic rescheduling, we have partnered with Fetch.ai to provide every MOBIX user with their own personal agents. To enable this, we connect you to the Fetch.ai Agentverse once to generate your secure credentials. Private keys never leave your device!

6. Gleam.io (third-party service provider)

We are using Gleam.io as a tool to increase awareness for the MOBIX wallet and to expand our user base. To sign up, you will only require a MOBIX address. Please keep in mind, that all transfers are publicly visible on the Fetch.Ai Blockchain via their block explorer. To keep your main wallet private, we recommend using a newly created MOBIX address to make correlation between your main account and your social media impossible.

Interacting over our Gleam.io campaign with the MOBIX Twitter account, in the form of following and retweeting, will provide MOBIX as well as Gleam.io the possibility to connect your wallet address with your Twitter account. Further, by signing up for our newsletter, your email is submitted to MOBIX. We ensure that we never store or link your personal identifiers, e.g. email address and twitter account, to your fetch address. However, as mentioned above, we recommend the usage of a new address to keep your main address private.

Glossary

Personally Identifiable Data - Data that contains personal direct and indirect identifiers.
Pseudonymous Data - Data from which identifiers are replaced with artificial identifiers, or pseudonyms, that are held separately and subject to technical safeguards.
De-Identified Data - Data from which direct and indirect identifiers have been removed
Anonymous Data - De-Identified Data where technical safeguards have been implemented such that data can never be re-identified.

Links:
https://dsearls.medium.com/a-privacy-manifesto-e475d4d8792a
➔ https://cyber.harvard.edu/projectvrm/Privacy_Manifesto
https://dictionary.cambridge.org/dictionary/english/privacy
https://en.wikipedia.org/wiki/Privacy_by_design
https://www.bclplaw.com/en-US/insights/at-a-glance-de-identification-anonymization-and-pseudonymization-1.html