Citopia Data Privacy Protection

What is Personally Identifiable Information (PII)?

Global Data Protection Regulation (GDPR) in the EU, and similarly the California Consumer Privacy Act (CCPA), define personal data as any information relating to an identified or identifiable natural person ('data subject'). Article 4 no.1 in GDPR defines an identifiable natural person as "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Recital 26 of GDPR elaborates on what constitutes identifiability like so: "to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". Data that enables the linkage of information to an individual allowing their identification can constitute personal data such as an IP or a blockchain address (any information that allows for identification).

Entities in Data Privacy Protection and Citopia's Role

Entities in the data privacy protection in the GDPR as defined as follows:

- A **data processor** is a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller. (Art. 4 no. 8 GDPR)
- A **data controller** is a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. For Citopia this would be California and Federal Laws. (Art. 4 no. 7 GDPR)

Citopia can be classified as a data processor because it is a federated Web3 marketplace where providers (e.g. enterprises and transit agencies) can offer B2B and B2C services. While Citopia offers users and enterprises Self-Sovereign Digital Twins (SSDTs) as a service, it has no access to the information stored in the SSDTs. Citopia may determine the means of data processing but it does not determine the purpose of data processing. Only the data controller can authorize data processing and determine its purpose.

How Does Citopia Maintain PII?

To understand how Citopia maintains data privacy, it is important to highlight how PII can be exposed. Firstly, PII can be exposed if it is stored. Therefore, the minimum set of PII should be stored only, if necessary. PII is also vulnerable to being exposed if the data controller or processor has not adopted proper pseudonymization or, better anonymization, techniques. Lastly, PII can be extracted if the correlability between data elements makes the data subject identifiable, meaning that data elements that can be related through statistical or other means allowing for the identification of the data subject. For example, the combination of name and address or unique identifiers tied to name, address or phone number can be used to obtain personal data.

As a data processor, Citopia processes different types of data and uses W3C-compliant Decentralized

Identifiers (DIDs) and Verifiable Credentials (VCs), along with zero-knowledge proofs (ZKPs) and other pseudonymization techniques, to ensure that PII is not exposed.

API service endpoints

Citopia processes API service endpoints in DID documents to enable service discovery, multi-party coordination, and business automation in the federated Web3 marketplace. API service endpoints are links which are only accessible by authorized entities and do not contain PII. Citopia architecture involves a two-way handshaking process to facilitate secure data exchange where only authorized entities can access the data via an authorized access token through a double-encrypted connection. Domain names in API service endpoints may contain identifiable information; however, this is strictly the responsibility of the providers.

User and service provider DIDs

Citopia processes user and service provider DIDs for onboarding, transactions, and multi-party coordination. DIDs do not contain PII but link to onboarding information, which is PII that is maintained in the owner's SSDT and is not stored by Citopia. This is done by anchoring the DID on-chain so that it is not visible to Citopia but only to the owner of the DID. It should be noted that user and service provider DIDs can be considered PII outside of the context of Citopia due to correlability.

Sufficiently pseudonymized hash of invoice VCs

Citopia stores the sufficiently pseudonymized hash of invoice VCs only in the Mobility-as-a-Service (MaaS) use case in order to maintain the accounting ledger for payments to service providers. This hash is linked to the service provider's DID only. The use of pseudonymized hash prevents Citopia from correlating data stored by Citopia with end user/ service provider personal or organizational data.

Aggregate of anonymized trip data

Citopia processes the aggregate of anonymized trip data for the use of service providers. For instance, aggregated anonymized trip data can be used to improve connectivity over various networks. Service providers will be responsible for providing data retention policies to Citopia regarding gathering aggregated data. Aggregated trip data may contain PII. Citopia prevents this PII from being exposed by extracting it in multiple steps. Each trip leg (mode of transit) is processed by a different Citopia node. User DIDs are removed from anonymized trip data and ZKPs are used to ensure data privacy, integrity, and verifiability. This way neither the service provider nor Citopia can identify PII from the anonymized trip data.

Sufficiently pseudonymized hash of Citopia Membership VCs

Citopia also stores the sufficiently pseudonymized hash of Citopia Membership VCs to enable users and service providers to use Citopia's federated Web3 marketplace. This hash is linked to the service provider's or user's DID only. The use of pseudonymized hash prevents Citopia from correlating data stored by Citopia with end user/ service provider personal or organizational data.