sovrin
identity for all

Innovation Meets Compliance

Data Privacy Regulation and Distributed Ledger Technology

AUTHORED BY: THE SOVRIN FOUNDATION
V.1.0 PUBLISHED JANUARY 2020

I. Introduction

This Position Paper describes whether and how the General Data Protection Regulation (GDPR) applies to us, the Sovrin Foundation, in our role as an administrator and participant in the Sovrin Network. We also assess whether and how the GDPR applies to other participants in the Sovrin Network, including the Stewards, Transaction Authors, Transaction Endorsers, Agencies, Developers, Holders, Issuers, and Verifiers.[1] The purpose of this Position Paper is to inform participants of their likely roles with respect to GDPR and is not intended to provide compliance advice for participants when they interact with data subjects. However, by connecting activities to the roles listed in the GDPR (e.g., data controller, data subject, data processor), we hope that this Position Paper can serve as a starting point for Sovrin Network participants in understanding their regulatory obligations. Although this Position Paper explicitly addresses only the GDPR, it is exemplary of our approach to data protection regulations across all jurisdictions.

The analysis of any specific use case or application of Distributed Ledger Technology (DLT) in the context of GDPR relies on facts and circumstances, which, in this case, includes the technical architecture of the Sovrin Network.[2] Some of these technical details are still under design and development; therefore, the scope of this analysis is limited to how the Sovrin Network is designed as of the date of this Position Paper. Specifically, the analyses, conclusions, and recommendations in this Position Paper do not take into account potential changes to the Sovrin Network and/or any additional projects or ventures in which the Sovrin Foundation may be involved, including the development or potential launch of a token.

Note that references to “natural persons” and “data subjects” in this Position Paper assume that these are natural persons and data subjects in the European Union, for the purposes of our analysis.

PLEASE NOTE: THE INFORMATION PROVIDED BELOW IS FOR INFORMATIONAL PURPOSES ONLY AND MAY NOT BE RELIED UPON BY ANY PARTY AS LEGAL ADVICE. PARTICIPANTS IN THE SOVRIN NETWORK SHOULD CONTACT THEIR COUNSEL TO OBTAIN ADVICE WITH RESPECT TO THE POTENTIAL APPLICABILITY OF THESE, AND OTHER LAWS, TO THEIR INTERACTION WITH THE SOVRIN NETWORK.

a. Key Takeaways Based on Current Implementation

Generally, when participants interact with personal data of a data subject in the EU (e.g., the Credentials or Proofs of another participant), they may be subject to the GDPR.[3] In contrast, if no personal data is transacted via the Sovrin Ledger Layer, participants in the Sovrin Ledger Layer are likely not subject to GDPR. The Sovrin Foundation designed the Sovrin Ledger Layer to facilitate conformance with GDPR by restricting data on the Sovrin Ledger to approved transactions that do not contain any personal data (at least during the

Permissioned Write Access Phase, which is discussed more below), as outlined by the Sovrin Foundation's governance policies and rules known as the Sovrin Governance Framework.

In its current implementation, the primary use of the Sovrin Ledger Layer is for templates, standardization, public notification, and the public display of information related to legal entities. These data types and their use cases are unlikely to include personal data, and therefore those entities that maintain, design, or write to the Sovrin Ledger are unlikely to have GDPR compliance obligations related to their use of the Sovrin Ledger. Furthermore, only legal entities may currently participate in writing transactions, making even the public addresses of Sovrin Ledger participants unlikely to be personal data.

In contrast, participants at the Credential Exchange Layer are likely to be subject to the GDPR because of their handling of personal data in the form of Credentials. Similarly, participants in the Agent-to-Agent Layer that assist in the transmission of Credentials (including hashed Credentials) are also likely to have obligations under the GDPR.

The Sovrin Foundation only participates at the Sovrin Ledger Layer. Therefore, the Sovrin Foundation and other participants in the Sovrin Ledger Layer are likely not subject to the GDPR as no personal data is currently permitted to be written to the Sovrin Ledger (assuming that all participants in the Sovrin Ledger Layer comply with the Sovrin Governance Framework).

b. Looking Forward

The Sovrin Foundation intends to deploy the Sovrin Network in two phases: the first being Permissioned Write Access where only approved Transaction Authors that are legal entities may write non-personal data transactions to the Sovrin Ledger and the second being Public Write Access where the Sovrin Foundation intends to open up the Sovrin Ledger to all Transaction Authors, including natural persons.

If natural persons are permitted to write to the Sovrin Ledger Layer in the future under Public Write Access, GDPR obligations will likely apply to participants in the Sovrin Ledger Layer since transactions will identify or be identifiable to a natural person (unless an exemption applies). Given the implications of allowing natural persons to interact with the Sovrin Ledger Layer, the Sovrin Foundation and each Sovrin Network participant's compliance obligations under the GDPR warrant deeper discussion and analysis outside the scope of this Position Paper. Given the fundamental properties of blockchain technology, we are likely to encounter compliance hurdles, but we are nonetheless committed to adapting the Sovrin Ledger Layer to comply with the obligations imposed by the GDPR to the extent possible.

To address some of these compliance hurdles, the Sovrin Foundation has already implemented various compliance strategies, such as requiring all processors in the Sovrin Network to execute data processing agreements with the Sovrin Foundation that meet the requirements of Article 28 of the GDPR, and is working closely with regulators and other key stakeholders in the EU to educate them about the Sovrin Network and self-sovereign identity. Because the regulatory landscape that governs the application of the GDPR to DLT use cases is in flux and the application of the law so often depends on complex technical architecture, we believe that the Sovrin Foundation has an opportunity to influence the development of the regulators' views regarding how best to regulate self-sovereign identity ecosystems.

The remainder of this Position Paper analyzes the application of the GDPR to the Sovrin Network based on its current implementation - that is, under Permissioned Write Access.

II. Description of the Sovrin Network

This section provides an overview of the Sovrin Network, starting with a description of the layers of the Sovrin Network and a short account of the operations of each layer.[4] We then explain the details for each of the primary Sovrin Network participants and their activities.

a. The Layers of the Sovrin Network

The Sovrin Foundation provides a global public utility in the form of the Sovrin Network that enables self-sovereign digital identity for all people and organizations. Each is known as an Identity Owner.[5] Each Identity Owner has the freedom to collect and store his or her own digital credentials in a personal digital wallet in the same way as he or she would carry analog credentials (e.g., a physical driver's license) in a physical wallet. Self-sovereign identity also enables Identity Owners to decide how and with whom to share these digital credentials, with the advantage that a third-party central authority cannot take away, sell, or otherwise act with respect to the Identity Owner's credentials without his or her approval.

The Sovrin Network is comprised of three key layers of technology from highest (closest to the end-user) to lowest (farthest from the end-user): (1) the Credential Exchange Layer, (2) the Agent-to-Agent Layer, and (3) the Sovrin Ledger Layer, each of which functions to enhance participant privacy by compartmentalizing and limiting access to personal data to the extent possible.[6] In this section, each layer of the Sovrin Network is described to the extent relevant to the GDPR analysis.

i. The Credential Exchange Layer

At the Credential Exchange Layer, each Identity Owner has a digital wallet ("Wallet")—typically an app running on a smartphone, tablet, desktop, or other local device—that holds Credentials containing certain information about that Identity Owner (e.g., a claim that the Identity Owner is of legal driving age). Credentials can either be issued by a third party, called an Issuer, or self-issued by the Identity Owner. As illustrated in Figure 1 below, once a Credential is created, it can then be verified by a third-party Verifier in order to make a trust decision about an Identity Owner (e.g., whether the Identity Owner is of legal driving age). To do this verification, the Verifier reads the Issuer's public key from the Sovrin Ledger (below) and uses it to verify the Issuer's digital signature on the Credential.

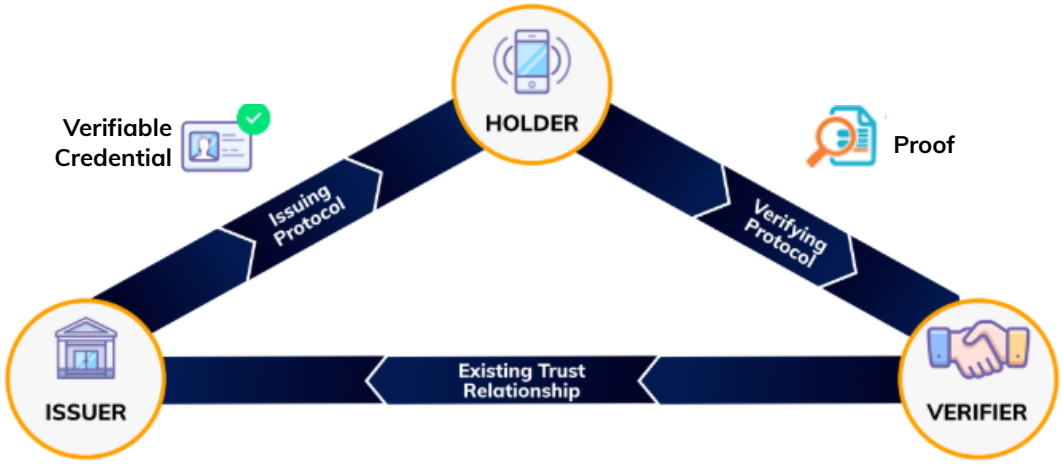

Figure 1 - Credential Exchange Layer Example

The Identity Owner owning the Wallet that contains a Credential is called a "Holder" of that Credential. It is also possible for a Holder to hold the Credential of another natural person (e.g., when acting as a Guardian) or of a business (e.g., when acting as a Credential Registry). Identity Owners can exchange Credentials through the Sovrin Network but do not interact directly with the Sovrin Ledger to do so. Instead, transactions at the Credential Exchange Layer occur entirely off-chain in peer-to-peer interactions.

ii. The Agent-to-Agent Layer

At the Agent-to-Agent Layer, Identity Owners enter into peer-to-peer Connections using specialized "Agent" software. This is the layer where Credentials can be privately transacted and verified between peers off-chain. Agent software developers build local clients, which may be downloaded to a device referred to as Edge Agents, and cloud-based clients, called

Cloud Agents, to facilitate Connections. Edge Agents are always operated locally by Identity Owners. Cloud Agents can be hosted directly by Identity Owners or hosted on behalf of Identity Owners by third parties known as Agencies.

As shown in Figure 2 below, the Agent-to-Agent Layer runs parallel to, but entirely separate from, the Sovrin Ledger Layer and Credential Exchange Layer, and data from this layer is never written to the Sovrin Ledger, even in hashed or encrypted form.

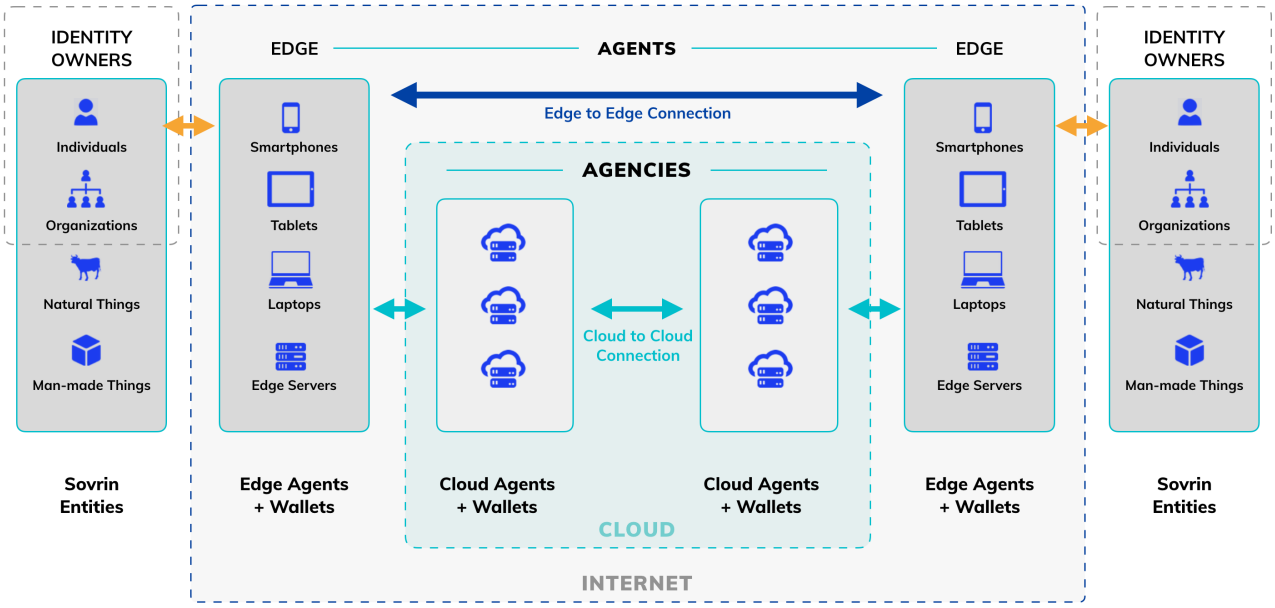

Figure 2 - Agent-to-Agent Layer Example

To establish a Connection, the two Agents each automatically generate a cryptographic key pair and compute a unique decentralized identifier, a Private DID [7], from that. This private DID is used to create and secure the Connection. Each Private DID resolves to a DID Document that contains the metadata needed to prove ownership and control of a Private DID, as well as a Service Endpoint, such as a URL or IP address. The Service Endpoint of each peer's Private DID is a network address that allows his or her Agents to communicate privately with one another separate from the Sovrin Ledger.

Private DIDs are a type of identifier designed to be fully under the control of the Identity Owner and not dependent on a centralized registry. A private DID is a pairwise identifier unique to each relationship between peers. For example, if a Holder (e.g., an individual) establishes a Connection with a Verifier (e.g., an online merchant), the Holder's and Verifier's Agents automatically create a unique Private DID for that relationship that can be used by the Holder and Verifier to securely and privately communicate with each other in the context of that relationship. Notably, each Private DID is only discoverable in the context of a specific pairwise relationship and is only known to the participants in that relationship. Private DIDs are also never stored on the Sovrin Ledger. Contrast this with the status quo where the

individual would sign in to the online merchant's website through a universal identifier that is utilized in multiple relationships (e.g., an email address) which can be used to track the individual.

iii. The Sovrin Ledger Layer

The Sovrin Ledger Layer, which is the only layer that runs on a blockchain, is the most public layer as it is designed to be a global ledger and is therefore readable by anyone. When used in accordance with the Sovrin Governance Framework, the Sovrin Ledger Layer will promote data privacy by limiting the transmission and storage of personal data. As shown in Figure 3 below, the Sovrin Ledger is the base layer of the Sovrin Network.

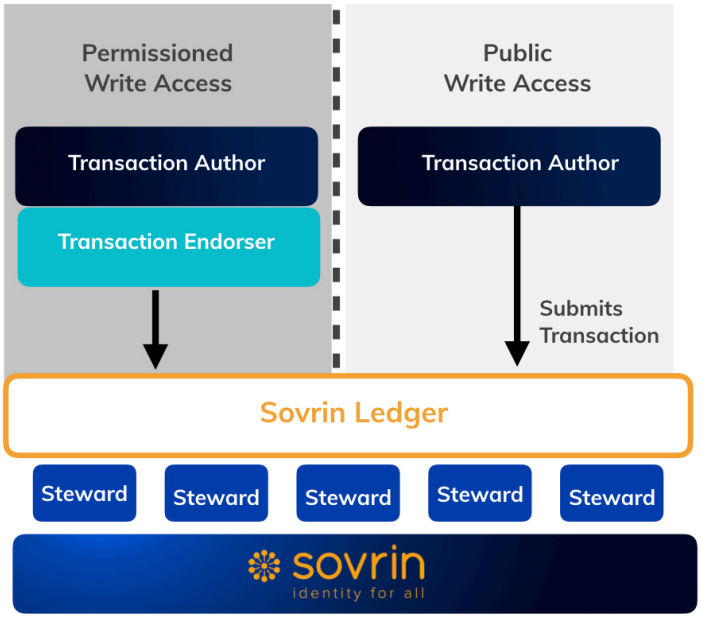

Figure 3 - Sovrin Ledger Layer Example

The only types of information that are written to the Sovrin Ledger are the following:

(1) **Schema** means the machine-readable format for specific attributes that can be used in a Credential (e.g., how to express a Holder's attributes in a machine-readable way, such as a Holder's age, date of birth, passport number, etc.). Although Schemas provide formatting for Credentials, it is important to emphasize that Schemas are not Credentials themselves and are not related to any natural person. Figure 4 shows an example Schema for a degree from a university. Note that the Schema in Figure 4 does not contain any information about a specific degree but provides a template for others to reference for creating Credentials of this type.

.

```
"ver": "1",
"txn": {
    "type": "102"
    "protocolVersion": 1,

    "data": {
        "ver": 1,
        "data": {
            "primary": {
                ...
            },
            "revocation": {
                ...
            }
        },
        "ref":95,
        "signature_type": "CL",
        "tag": "some_tag"
    },
    "metadata": {
        "digest": "fa431da357aa81f7b6b513abfac44cf562428c6a3222be518c92e5edd4949296",
        "reqId":1538510026756382700,
        "from":"HR6vs6GEZ8rHaVgjg2WodM"
    },
},
"txnMetadata": {
    "txnTime": 1538509962,
    "seqNo": 96,
    "txnId": "HR6vs6GEZ8rHaVgjg2WodM:3:CL:Degree:some_tag"
},
"reqSignature": {
    "type": "ED25519",
    "values": [{
        "from": "HR6vs6GEZ8rHaVgjg2WodM",
        "value": "62VjqA7zCwdZh983mDkERBefGoXvRGcdH4uUxKaVEdegxx8VppGMKDf4qWHb3CTSWVU5x69ga5re4pjC3qmtH75P"
    }]
}
```

Figure 4 - Schema Example

(2) Credential Definitions mean the specific, machine-readable formats that Issuers create, which reference one or more Schemas and specify the Issuer's public key that is used to digitally sign Credentials that use this Credential Definition. Credential Definitions ensure that Credentials issued by a particular Issuer fit a certain format and are interoperable across multiple Issuers, Holders, and Verifiers. For example, a Credential Definition might specify that one Claim in the Credential (i.e., a specific Attribute data type) is a true/false statement that the subject of the Credential is over 21 years of age. A Credential Definition can incorporate Claim definitions from multiple Schemas. Although Credential Definitions provide the formatting for a Credential, it is important to emphasize that they are also not Credentials themselves and are not associated with any natural person. Please see Figure 5 for a Credential Definition for an Issuer using the Schema in Figure 4 above. Note that the Credential Definition in Figure 5 does not contain any information about a particular natural person but does reference the signature of the Issuer ("reqSignature") and a Schema ("ref").

Figure 5 - Credential Definition Example

(3) **Participants and Roles** mean transactions submitted to the Sovrin Ledger to add or modify the list of entities that can act as Transaction Authors and write transactions to the Sovrin Ledger. These transaction requests take a variety of forms but relate only to the permissioning of entities that act as Transaction Authors on the Sovrin Ledger.

(4) **Revocation Registries** mean the cryptographic data structures written to the Sovrin Ledger by an Issuer that allows an Issuer to change the status of a Credential (e.g., revoke a Credential) without revealing the owner of the Credential or the content of the Credential. For example, if a Holder's Credential stating that he or she has a valid driver's license needs to be revoked, this can be done through the Issuer's corresponding Revocation Registry. The Sovrin Foundation created Revocation Registries to address the challenge of revoking Credentials in an efficient way that is respectful of privacy. Revocation Registries use special cryptography so that it is not possible by reading the Revocation Registry data to determine which Credentials have been revoked. Thus, only Holders and Proof recipients can know the underlying data subject related to the revocation.

(5) **Anywise DIDs**[8] mean DIDs that permit the creation of a non-reciprocal relationship rooted in the identity of one party in a pairwise relationship, where the second party does not need to reveal its identity to refer to the first party. Legal entities may become Issuers of Credentials by writing an Anywise DID to the Sovrin Ledger so that an Identity Owner may reference that Issuer without revealing his or her own identity. For example, if an Identity Owner wishes to contact a government agency and establish a Connection, the Identity Owner would first look up the government agency's Anywise DID on the Sovrin Ledger so that his or her Agent could directly connect with the government agency's Agent off-chain using the Agent-to-Agent Layer. The new Connection formed

between the Identity Owner and the government agency uses Private DIDs as described above, is entirely private to these two parties, and does not involve the Sovrin Ledger.

b. The Participants in the Sovrin Network

This section offers a summary for each participant in the Sovrin Network.

i. Credential Exchange Layer Participants and Activities

There are three primary participants in the Credential Exchange Layer: Holders, Issuers, and Verifiers..

1. Holders

Holders are natural persons or entities that store Credentials in their Wallets for use in the Sovrin Network. The Holder can be the Identity Owner that is the subject of the Credential, but a Holder can also be a third party that is not the subject of the Credential. For example, a Guardian can administer a Dependent's Identity Data, such as a birth certificate, where the Identity Owner is a baby, and therefore a Dependent, and both parents are Holders and therefore Guardians. Holders may either issue their own Self-Issued Credentials or receive Credentials from external Issuers. When a Verifier requests a Proof of a Credential from a Holder, the Holder chooses whether to approve the request. If approved, a Proof of the Credential is provided by the Holder to the Verifier.

2. Issuers

Issuers are natural persons or organizations that issue Credentials to Holders. An Issuer can be an Organization (e.g., the Department of Motor Vehicles that issues a Credential that a person has a valid driver's license) or an Identity Owner who self-issues Credentials (e.g., I claim that I graduated from college). Under Permissioned Write Access, Issuers who enter into the Transaction Author Agreement with the Sovrin Foundation must use a Transaction Endorser to publish Anywise DIDs, Schema, Credential Definitions, and Revocation Registries to the Sovrin Ledger.

3. Verifiers

Verifiers are Entities that request Proofs from Holders in order to make a trust decision about the subject of their request. Note that Verifiers do not request the actual Credential, but rather a Proof of a specific set of Claims from one or more Credentials, where the data is proven using ZKP (Zero-Knowledge Proof) cryptography as further described below. ZKPs allow proof of one or more Claims from one or more Credentials without revealing the underlying Credential or Claim data if that data is not actually required by the Verifier. Note that Verifiers may also serve as Issuers and Holders—almost all participants in the Sovrin ecosystem will serve in one or more of these roles.

ii. Agent-to-Agent Layer Participants and Activities

There are three primary participants in the Agent-to Agent Layer: Identity Owners, Developers, and Agencies.[9]

1. Identity Owners

Holders, Issuers, and Verifiers are all Identity Owners that can use Agents. Identity Owners interact with Agents to form Connections, exchange Credentials, and perform other secure private transactions.

2. Developers

Developers design and release hardware or software providing the functionality of any component of the Sovrin Network, including Nodes, Agents, and Wallets.

3. Agencies

Agencies are service providers that host or provide Agent software for Identity Owners. Agencies that provide Cloud Agents have specific Service Endpoints used for Connections. However, Edge Agent software does not include Service Endpoints for Identity Owners because: a) Edge Agents, such as mobile devices may not always be online, and b) such a Service Endpoint may compromise the privacy of Identity Owners by revealing their IP address or other location information.

iii. Sovrin Ledger Layer Participants and Activities

Besides the Sovrin Foundation, there are three other primary participants in the Sovrin Ledger Layer: Stewards, Transaction Authors, and Transaction Endorsers.[10]

1. Stewards

Stewards are Organizations approved by the Trustees to operate a Node to maintain the Sovrin Ledger. Stewards must contractually agree to the Sovrin Steward Agreement and the Steward Data Processing Agreement with the Sovrin Foundation that commits them to terms and conditions relating to confidentiality, intellectual property, and data privacy, among other terms and conditions. Stewards who agree to the Transaction Author Agreement and Transaction Endorser Agreement may also serve as Transaction Authors and Transaction Endorsers.

2. Transaction Authors

Transaction Authors are Entities who write Transactions to the Sovrin Ledger. All Transaction Authors must agree to the Transaction Author Agreement. Transaction Authors may only write Transactions to the Sovrin Ledger that fit into one of the five categories of information listed above in Section II.a.iii.

3. Transaction Endorsers

A Transaction Endorser is an Organization that endorses a Transaction from a Transaction Author by digitally signing it so it will be accepted by a Node operated by a Steward at the Sovrin Ledger Layer. Transaction Endorsers must be authorized by the Sovrin Foundation to endorse Transactions from a Transaction Author by entering into the Transaction Endorser Agreement with the Sovrin Foundation. Transaction Endorsers must endorse all Transactions submitted to them by a Transaction Author unless it is prohibited to do so by the terms of the Transaction Endorser Agreement.

The relationship between Sovrin Foundation and these roles and agreements at the Sovrin Ledger Layer are captured in this diagram from the Sovrin Glossary.

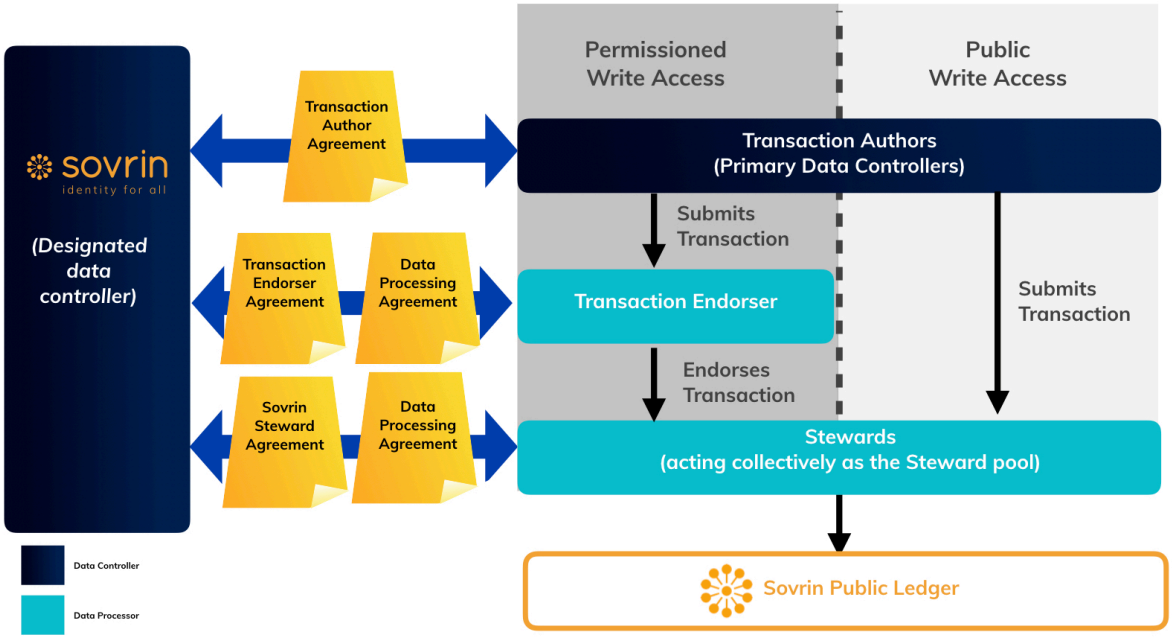

Figure 6 - Roles and relationships at the Sovrin Ledger Layer

The two different columns for Permissioned Write Access and Public Write Access reflect different sets of policies for how transactions may be written to the Sovrin Ledger as defined in the Sovrin Ledger Access Policies document of the Sovrin Governance Framework.

III. Overview of the GDPR

Before we analyze whether and how the GDPR applies to the Sovrin Network, in this Section III, we provide an overview of the GDPR, how the GDPR applies to DLT generally, and key GDPR definitions.

Broadly speaking, the GDPR applies to the processing of personal data of natural persons in the EU, regardless of whether the processing takes place in the EU or not. The GDPR applies

to organizations in the EU and extraterritorially to organizations outside of the EU who monitor, or offer goods or services to, individuals in the EU. [11]

a. Key GDPR Definitions[12]

Below are key definitions from the GDPR that inform this Position Paper.

- anonymous refers to information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.[13]
- controller means the 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.
- processor means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
- data subject means the identifiable natural person about whom personal data is collected.
- processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is 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.
- pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

b. Key GDPR Actors

Under GDPR, there are three main actors: **controller**, **processor**, and **data subject**. The category into which a participant falls under the GDPR turns on variables such as:

- Whether the type of data they are processing is defined as "personal data" under the GDPR;
- The amount of control they have to determine the purposes and means of processing personal data; and/or
- Whether they are subject to any exemptions to the GDPR.

The controller exerts control over how the personal data of the data subject is processed and by which processors, if any. The processor must only process personal data in accordance with instructions from the controller. While a processor also has independent compliance obligations (such as having appropriate security measures in place and notifying controllers if they have a breach), primary GDPR liability and compliance obligations remain with the controller. Multiple parties can be controllers or processors to the same personal data.

A controller and a processor must be a natural or legal person, public authority, or body. Therefore, the controller and the processor cannot be purely technology (e.g., software). As an example, a smart contract or a blockchain in and of itself cannot be a controller or a processor, whereas the entity that controls the smart contract or blockchain, such as the developer or a node, can be a controller or processor depending on a variety of factors as explained below. Additionally, the data subject must be a natural person. Therefore, things cannot be data subjects and cannot have personal data, but natural persons that own or use things, such as mobile devices, can be data subjects and can have their personal data processed

c. GDPR in the Context of Self-Sovereign Identity and Blockchain

i. Tension Between Blockchain and GDPR

Many in the technology industry have claimed that DLT and the GDPR are incompatible or, at the very least, are in serious conflict with one another. This may be because applying the GDPR to DLT is like fitting a square peg into a round hole due to the vastly different data models assumed by the drafters of the GDPR and how DLT generally handles data. As shown in Figure 6, under the dominant data model that currently exists, participants often have to create accounts which interact with third-party intermediaries, who collect and store users' data and decide how to handle that data, oftentimes without the users' knowledge. These third-party intermediaries (e.g., large technology companies) may exercise considerable power over users. Therefore, when EU regulators first started drafting the GDPR in 2012, centralized client-service network relationships strongly influenced their thinking.

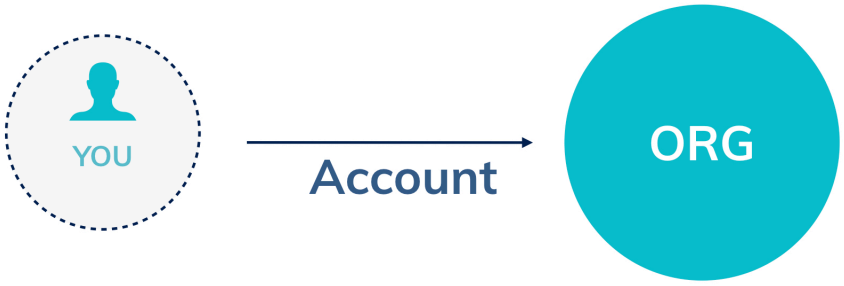

Figure 7 - Traditional Data Relationship

In contrast, one of the fundamental features of DLTs (particularly, DLT employed in public-permissionless blockchains) is that it is decentralized, meaning there is no centralized authority that determines how and where data is stored, processed, or otherwise used. The decentralization of collection and storage of data across all nodes running an instance of the ledger upends traditional models of collecting and storing personal data by removing third-party intermediaries. As shown in Figure 7, under a disintermediated data model like the Sovrin Network, data transactions can be peer-to-peer without any third-party intermediary.

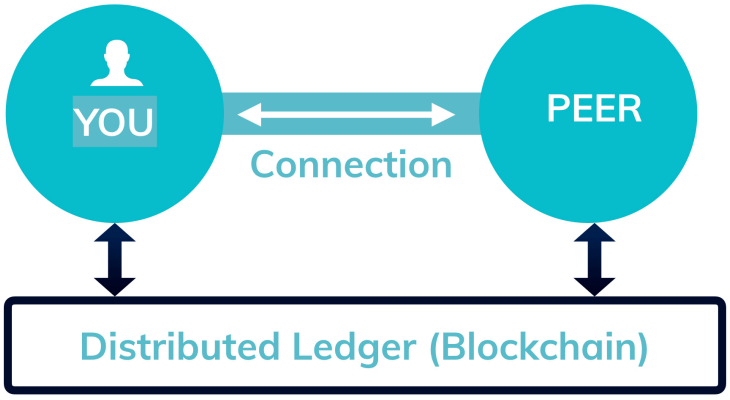

Figure 8 - Peer-to-Peer Data Relationship

ii. Determining the Controller, Processor, and Data Subject in a Blockchain System

Under this disintermediated and decentralized model, it may be difficult, if not impossible, for data protection authorities to identify which participants in a blockchain system are controllers, processors, or data subjects. Nonetheless, EU government entities, such as France's Commission Nationale de l'Informatique et des Libertés (CNIL) and the European Parliamentary Research Service Scientific Foresight Unit, as well as European Commission-affiliated industry groups, such as the EU Blockchain Observatory and Forum (EU Blockchain Forum), have released reports or written guidance on GDPR as applied to

blockchain systems. These reports generally approach the analysis of GDPR to blockchain solutions by identifying whether various participants in the applicable system are classified as a controller, processor, or data subject.

In fact, the EU Blockchain Forum states in its thematic report "Blockchain and the GDPR" that "[a]s far as the GDPR is concerned, it must be possible to identify a data controller."[14] However, the EU Blockchain Forum does not clarify what happens if it is not possible to identify a controller, such as in a public, permissionless blockchain.

The CNIL's recent guidance also did not propose any regulatory conclusions for situations where there is no controller; in fact, the CNIL is still undertaking an in-depth analysis on this question.[15] The CNIL recommends that organizations carefully examine whether blockchain is the most suitable technology if its use will lead to compliance challenges with the GDPR. The absence of concrete guidance from EU regulators on how to resolve GDPR compliance hurdles has left many blockchain developers in a state of uncertainty.

Nonetheless, with the regulatory guidance currently available, it is clear that we must start the GDPR analysis by figuring out which participants in the blockchain system are controllers, processors, and data subjects. Below are some fundamental principles to aid our analysis:

- GDPR does not apply if there is no processing of personal data of a data subject.
- Without a data subject, there can be no controller. Without a controller, there can be no processor.
- The more concentrated the ability of participants to direct the architecture of the blockchain and the more control those participants have to determine the means and purposes of processing, the easier it becomes to identify a controller(s).
- Conversely, the more diffuse the ability of participants to direct the architecture of the blockchain and the less control that participants have to determine the means and purposes of processing, the harder it becomes to identify a controller(s).
- The amount of control participants have to direct the architecture of a blockchain system may depend on its governance model. A public, permissionless blockchain is often the most open, and therefore, presents the most difficulties in identifying the controller and processor.

There are four primary types of blockchain governance models:

Access	Validation: Permissionless	Validation: Permissioned
Public	• Anyone may operate a node or validate transactions • Anyone can create transactions on the ledger (e.g., Bitcoin, Ethereum)	• Permission from some governing entity is required to operate a node or validate transactions • Anyone can create transactions on the ledger (e.g., Sovrin)
Private	• Anyone may operate a node or validate transactions • Single centralized organization restricts ability to write to ledger, read permissions ether public or restricted (e.g., Hyperledger Sawtooth)	• Permission from some governing entity is required to operate a node or validate transactions • Single centralized organization restricts ability to write to ledger, read permissions ether public or restricted (e.g., Ethereum Enterprise, Hyperledger)

Figure 9 - Blockchain Governance Models

iii. Digital Identity Under the GDPR

EU regulators recognize these inherent tensions between the GDPR and blockchain, but also acknowledge that specific use cases of blockchain, particularly self-sovereign identity solutions, are compatible in spirit with the GDPR. *It is worth emphasizing that the philosophical underpinnings of blockchain and GDPR are aligned (e.g., giving individuals control over their personal data).*

In fact, the European Parliament passed a non-binding resolution on October 3, 2018 requesting the EU to take an innovation-friendly approach to regulating blockchain. It specifically stated the following on self-sovereign identity and trust:

> *28. Underscores that DLT enables users to identify themselves while being able to control what personal data they want to share; notes that a wide range of applications can allow different levels of transparency, raising the need for applications to be compliant with EU law; stresses also that data in a public ledger are pseudonymous and not anonymous...*
>
> *32. Underlines that although DLT promotes self-sovereign identity, the 'right to be forgotten' is not easily applicable in this technology...*

> *33. Emphasizes that it is of the utmost importance that DLT uses are compliant with the EU legislation on data protection, and notably the General Data Protection Regulation (GDPR); calls on the Commission and the European Data Protection Supervisor (EDPS) to provide further guidance on this point[.][16]*

In July 2019, the European Parliamentary Research Service Scientific Foresight Unit published a comprehensive examination of the GDPR as applied to blockchain technologies ("STOA Report").[17] The STOA Report reiterates some of the issues identified in the CNIL guidance, but importantly includes policy suggestions for European regulators designed to address the incongruities in the GDPR when applied to blockchain. Specifically, the STOA report seeks further guidance from regulators on whether the "household exemption" can be invoked in relation to public and permissionless blockchains, whether anonymization is sufficient for satisfying erasure requirements, and whether a data subject can be a data controller for their own personal data. These and other questions remain unanswered.

Though difficult, DLT use cases can be designed to be compatible with the GDPR, provided that the use case is developed with privacy-protective design features baked into the way that it functions. Publicly-issued guidance, including from regulators such as CNIL, and market research firms, such as Forrester, shows the best practices for a GDPR-compatible permissioned DLT design include:

- Designing the system to prohibit or prevent personal data from being stored or referenced on-chain;
- Making sure that there is not reliance on encryption for on-chain data that could constitute personal data (quantum computing is a threat to all forms of encryption including methods used in DLT);
- Designing the blockchain such that on-chain hash information and metadata are capable of being rendered valueless (e.g., via deletion of off-chain data and destruction of keys and correlation to the extent possible);
- Delinking the identity of the key owner from the key belonging to that key owner (the signer of a transaction should not be identifiable as a natural person);
- Determining governance rules for participants in a permissioned DLT network to support GDPR accountability;
- Conducting privacy risk assessments for risk mitigation; and
- Engaging legal counsel early in development.[18]

d. Opportunity to Advocate for Interpretation of the GDPR that Fosters Growth of Self-Sovereign Identity as a Privacy Enhancing Tool

It is encouraging that EU regulators recognize the need for further guidance on the application of the GDPR to self-sovereign identity platforms. The Sovrin Foundation is in a unique position to advocate for a more flexible interpretation of the GDPR that fosters the growth of self-sovereign identity rather than hinders it.

A literal application of the GDPR to DLT may result in non-practical outcomes that are not in the public best interest nor consistent with the spirit and intent of the GDPR. For example, in a public, permissionless blockchain, anyone that downloads the appropriate software client can run a node and interact with the blockchain. Generally, nodes on a public, permissionless blockchain only store a copy of the ledger, can only view the encrypted or hashed data and cannot modify the data.[19] A node's role is generally limited to maintaining a copy of the blockchain and validating transactions based on a self-executing consensus algorithm. If node operators are deemed to be controllers, this may create a result that is impractical and administratively difficult to enforce. For example, it could mean that node operators (some of whom are individuals that are using their personal computers) are subject to the GDPR, despite not exercising any control over the purposes and means of processing personal data. It could also mean that node operators need to fulfill data subject requests such as the right to data rectification even though they cannot modify the data on the blockchain and therefore have no ability to fulfill the data subject request. When participants to a blockchain are transacting in a purely peer-to-peer manner and the only other participants are nodes that are essentially passive entities and have no ability to modify or read the data on the blockchain, it may not be consistent with the spirit of GDPR to treat all nodes as controllers.

The EU Blockchain Observatory states in its Blockchain and GDPR Report, "Public, permissionless blockchains represent the greatest challenge in terms of GDPR-compliance, because of their extremely distributed nature."[20] In contrast, it states "private, permissioned blockchain networks operated by consortiums of companies or government agencies, will find it easier to apply the letter of the GDPR." Public, permissioned blockchain systems (like the Sovrin Network) will fall somewhere in between.

The Sovrin Foundation intends to engage in multiple levels of regulatory process to educate EU regulators and lawmakers about DLT technology and to advocate for regulatory clarification, guidance, and where appropriate, change to accommodate self-sovereign identity solutions as an alternative to heavily-regulated approaches designed for traditional client/server data sharing architectures.

e. GDPR Applicability Decision-Tree

Now that we have covered the basics of the Sovrin Network and the GDPR, we will set forth a framework to determine whether the GDPR applies to the Sovrin Network and each participant therein. Below is a decision-tree that helps determine whether the GDPR applies. It is crucial to undertake this analysis with respect to each layer of the Sovrin Network, participant in the Sovrin Network, and activity of such participant. This is especially true because a participant's role in the Sovrin Network is dynamic. For example, an Issuer can be a controller while conducting one activity, and a processor while conducting another activity.

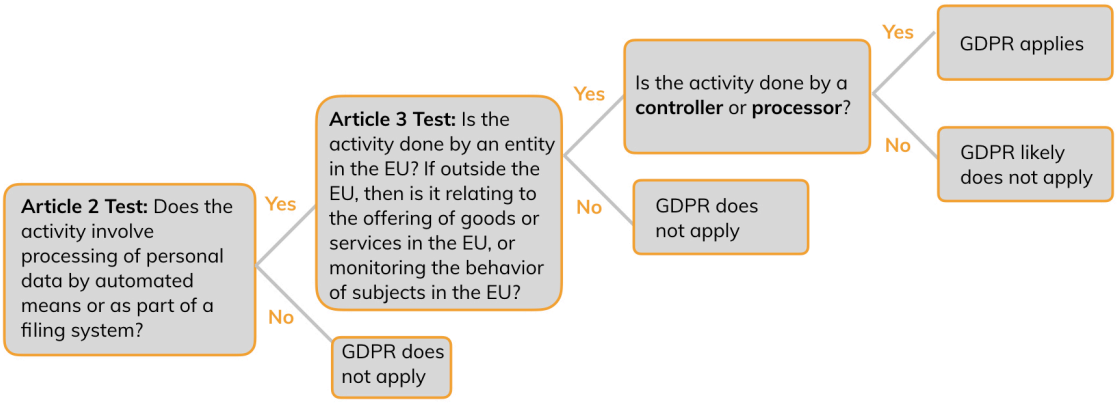

Figure 10 - GDPR Applicability Decision-Tree

f. Processing Outside the Scope of the GDPR

The GDPR does not automatically apply simply because the Sovrin Network is a global public utility accessible by people and organizations in the EU. There are two key ways that the GDPR may not apply to the activities of the Sovrin Foundation or the Sovrin Network.

i. No Personal Data is Processed

The GDPR governs the processing of personal data. Thus, it does not apply to aspects of the Sovrin Network that do not include the processing of personal data. For example, information that is purely about an organization (e.g., an Issuer's Anywise DID as long as the Issuer is not a natural person) that does not contain any personal data should fall outside the reach of GDPR.

Even though the Sovrin Governance Framework currently limits Transaction Authors and Transaction Endorsers to legal entities, only permits the five categories of non-personal data transactions listed in Section II.a.iii above to be written to the Sovrin Ledger, and pseudonymises all DIDs written to the Sovrin Ledger, the Sovrin Foundation only considers this exception narrowly because the definition of personal data under the GDPR is extremely

broad. Pseudonymous data is de-identified but can, with reasonable effort and the use of additional data (either publicly available or held but kept separate by the controller), identify a particular data subject. Pseudonymous data includes online identifiers provided by a data subject's devices, applications, tools and protocols (i.e., IP addresses, cookie identifiers, and radio frequency identifiers). Under the GDPR, pseudonymous data is still considered personal data that is subject to its protections, although the GDPR intends to "create incentives to apply pseudonymization" because it is viewed as helping to safeguard data subjects' rights and freedoms.[21]

In contrast to pseudonymous data, anonymous data is not considered personal data under the GDPR (although it may be still be governed by other EU privacy laws). Anonymous data cannot be used to identify any data subject even with other available data and the exercise of reasonable effort. Determining whether data is anonymous data requires a close technical analysis of the methods used to obfuscate the underlying personal data. The EU Blockchain Observatory states that the higher the reversibility and/or linkability risks, the less likely the data is anonymous. Reversibility refers to the likelihood that the applicable hashed or encrypted data, for example, can be reversed to reveal the underlying data, considering the technology available currently and expected to be available in the future. Linkability refers to the ability to recognize a pattern in the data to discover information about a natural person (e.g., correlations can be drawn from the hashed data, especially by combining it with other data, to reveal information about the subjects whose information is in the hashed data). Conversely, the lower the reversibility risk and linkability risk, the greater likelihood that the EU would consider the data to be anonymous[22].

The Court of Justice of the EU concluded that personal data is anonymous data if identification of the data subject is "practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant."[23] Working Party 29 stated that three criteria should be considered to determine whether information that has been anonymized can still be considered personal data[24]:

- Is it still possible to single out an individual?
- Is it still possible to link records relating to an individual?
- Can information be inferred concerning an individual?

ii. Household Exemption

The GDPR does not apply to any processing of personal data undertaken by a natural person "in the course of a purely personal or household activity."[25] These personal and household activities may include "correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities."[26] However, European courts, including the European Court of Justice ("ECJ"), have construed

this exemption narrowly, and the personal or household activities cannot be connected in any way to any professional or commercial activities for the exemption to apply.[27]

The CNIL applied the household exemption to conclude that a natural person who buys or sells Bitcoin, on his or her own behalf, is not a controller.[28] However, the STOA Report challenges the CNIL's interpretation in light of the ECJ's interpretation that the dissemination of information to an indefinite number of people using a blockchain network is inconsistent with the ECJ's strict interpretation of the household exemption.[29]

Notwithstanding the STOA Report's challenges to the CNIL interpretation of the household exemption, we believe that Identity Owners who are natural persons, and who access and use the Sovrin Network for purely personal or household activities (e.g., to authenticate their email accounts, social networking accounts, and other internet accounts) likely are not subject to the GDPR as controllers, although the controllers and processors of such data likely are subject to the GDPR.

One of the Sovrin Foundation's goals in developing the Sovrin Network is to tackle the antiquated model of using universal identifiers (like usernames and passwords) to authenticate one's identity. Our goal is to design the Sovrin Network in such a way that Identity Owners are exempt from the GDPR as long as they meet the strict household exemption criteria.

As a "self-sovereign" identity network, when Transaction Authors write data to the Sovrin Ledger themselves, they are acting as controllers of their own data. GDPR was not drafted with this concept in mind: it presumes that a controller exists to process or direct processing of someone else's data. However, when the Sovrin Network becomes truly "self-sovereign" such that no intermediary parties are necessary for natural persons to write their own transactions to the Sovrin Ledger, EU regulators may be convinced to view all self-sovereign participation as a "personal," or household activity" and therefore exempt under this exception. However, we believe this view is premature in the absence of regulatory clarity..

IV. Application of GDPR to Sovrin Network Participants and Activities

This section utilizes the framework described above to determine the applicability of the GDPR to the types of data, participants, and activities within each layer of the Sovrin Network.

a. Credential Exchange Layer Participants - Issuers, Verifiers, Holders

The first question is whether the Credentials themselves constitute personal data. Credentials typically include information related to data subjects (e.g., claims regarding date of birth or education). The underlying claim data contained in Credentials will likely be considered personal data under the GDPR. Although there may be encryption techniques

applied to Credentials to obscure the underlying personal data in the claim, the following analysis will assume that under most circumstances, the claim data, and therefore the Credentials themselves, constitute personal data.

If the type of data transmitted at the Credential Exchange Layer is personal data, participants in the Credential Exchange Layer are likely to have obligations under the GDPR, assuming that the other elements of the GDPR Applicability Decision-Tree discussed in Figure 9 are met and an exemption does not apply. Because participants may play multiple roles within the Credential Exchange Layer, it is infeasible to provide a conclusive determination regarding the applicability of the GDPR for each participant category. For example, the same Organization can play the role of Issuer when issuing a Credential to an Identity Owner (in the role of Holder), and the role of Verifier when requesting a Proof of that Credential (or any other Credential) from the Holder. Given the difficulty of definitively categorizing participants for the GDPR— Issuers, Verifiers, and Holders should consider the following:

i. Issuers

Issuers that offer Credentials to Identity Owners are likely to be controllers because in that instance, they are acting as the entity that determines the purposes and means of the processing of a Credential. However, Issuers that process an Identity Owner's requests for Credentials are likely to be processors as they are acting on behalf of the Identity Owner as the controller, in that instance. An Issuer can be a controller for some activities and a processor for others.

ii. Verifiers

Verifiers that request Credential Proofs from Identity Owners are likely to be controllers because they would be determining the purposes and means of the processing of a Credential. Typically, this purpose is to make a trust decision for a given Credential. Proofs from Holders that relate to natural persons are likely to be personal data, even though they do not contain the underlying Credential since the Proof is still "about" a natural person.

iii. Holders

The CNIL stated that a natural person that transacts data on a blockchain can be considered a controller if the transactions are "carried out as part of a professional or commercial activity, on behalf of other persons".[29] Therefore, if a natural person is not subject to the household exemption, he or she may be considered a controller under the GDPR because he or she determines what Credentials to hold and how to treat those Credentials (e.g., when acting on behalf of another Identity Owner or as an Issuer or Verifier for the Credentials of others).

b. Agent-to-Agent Layer Participants - Identity Owners, Developers, and Agencies

Similar to the Credential Exchange Layer, the information that is transmitted via the Agent-to-Agent Layer includes Credentials and therefore personal data. Accordingly, the analysis

regarding Credentials above also applies to the Agent-to-Agent Layer. Similarly, participants at the Agent-to-Agent Layer that are also participants in the Credential Exchange Layer (e.g., Identity Owners) are likely subject to the same obligations under the GDPR as they are at the Credential Exchange Layer. The analysis in this Section focuses on participants that do not operate at the Credential Exchange Layer, such as the Developers and the Agencies who host Identity Owners.

i. Developers

Developers may be subject to the GDPR to the extent that they operate a business that processes the personal data of data subjects in the EU. In circumstances where Developers simply produce Agent software but are not involved in handling the personal data transmitted through the Agents, they may not be subject to the GDPR. The CNIL stated in its recent guidance that "[r]egarding smart contracts, as for any software, the algorithm developer may simply be a solution provider or, when the said algorithm developer participates in the processing, may be qualified as a processor or controller depending on its role in determining the purposes of the processing."[31] Ultimately, a conclusive determination regarding the risk of whether a Developer is subject to GDPR depends on the particular functions of the Developer's software and/or the services the Developer offers.

ii. Agencies

Agencies may be subject to the GDPR depending on their role in managing and hosting interfaces that Identity Owners interact with in order to transmit personal data. The goal of Sovrin Network architecture is for Agency operators to not have any control over the data or activities of Identity Owners, whether personal data or not, but function only as data processors acting on behalf of those Identity Owners as data controllers. However, it is possible that agencies may be deemed to be controllers and/or processors depending on the exact nature of their processing. Therefore, Agencies must ensure that they carry out their GDPR obligations with respect to any EU data subject that uses their services.

c. Application of GDPR to Sovrin Ledger Layer Participant Activities

Under the Permissioned Write Access implementation of the Sovrin Network, the Sovrin Foundation has taken significant steps to avoid the transmission and/or storage of any personal data via the Sovrin Ledger. In fact, the Sovrin Governance Framework has followed Privacy by Design principles specifically to minimize the storage of personal data. This Position Paper analyzes the types of information that are stored and processed on the Sovrin Ledger and evaluates whether such types of information are personal data and therefore subject to the GDPR. Overall, we believe that the risk of personal data being processed at the Sovrin Ledger Layer is low, provided that Transaction Authors comply with the the Sovrin Governance Framework. However, there are no technical mechanisms that can completely prevent Transaction Authors from writing personal data directly to the Sovrin Network in violation of current Sovrin Governance Framework.

Ultimately, the eventual goal and vision of the Sovrin Foundation is to provide Public Write Access, thus empowering full self-sovereign participation by all Transaction Authors so

anyone is allowed to write transactions directly to the Sovrin Network themselves. Under Public Write Access when natural persons are permitted to serve as Transaction Authors, their Anywise DIDs, public keys and Service Endpoints are likely to constitute personal data subject to the GDPR. However, as noted previously, we intend to do additional work to engage with regulators and increase clarity as to the application of the GDPR to DLT and self-sovereign identity, prior to moving to Public Write Access.

i. Lookup, Discovery, and Verification of Anywise DIDs

Under the Permissioned Write Access policies, the Sovrin Ledger may be used for the lookup, discovery, and verification of Anywise DIDs belonging to Organizations (and not natural persons). As stated in the Sovrin Foundation's article "Sovrin: What goes on the Ledger?", the primary function of the Sovrin Ledger is to serve as a publicly-available registry that contains DIDs and their DID Documents. The DID Documents contain the metadata needed to prove ownership of the DID and the associated public keys, and to serve as a pointer to a Service Endpoint. The Identity Owner uses the Service Endpoint to contact the Organization's Agent and establish a unique pairwise connection between the Organization and the Identity Owner.

The Sovrin Ledger is analogous to a traditional phone book that is also used for lookup and discovery purposes, except that the use of DLT, Anywise DIDs, and the Agency-to-Agency Layer allows usage of this "phone book" without revealing any conventional identifying information. As a result, where the Sovrin Ledger Layer is used solely for lookup, discovery, or verification purposes of Organizations, there is a low risk that personal data is processed since Transaction Authors are restricted in the types of information that they can include in DID Documents and only Organizations are currently permitted to write to the Sovrin Ledger.

ii. Schema and Credential Definitions

The Sovrin Ledger may also be used for storing Schema, which are used by Issuers to create Credential Definitions written to the Sovrin Ledger. A Credential Definition is an instance of a Schema that includes attribute-specific public verification keys that are bound to an Issuer. Similar to Anywise DIDs, the use of Schemas and Credential Definitions on the Sovrin Ledger are unlikely to constitute personal data based on the nature of their use.

iii. Participants and Roles

So long as the Transaction Authors that are added to the Sovrin Ledger are Organizations (and not natural persons) and comply with the Sovrin Governance Framework and the Transaction Author Agreement, it is unlikely that such additions or modifications would constitute personal data. Furthermore, where natural persons are acting exclusively at the behest of a legal entity, the Node Addresses and Anywise DIDs of such Transaction Authors would not constitute personal data.

iv. Revocation Registries

When an Issuer of a Credential revokes a Holder's Credential, the Issuer may write to a Revocation Registry on the Sovrin Ledger to provide notice that a Credential has been revoked. In these instances, neither Credentials nor hashed representations of Credentials are ever written to the Sovrin Ledger. The Sovrin Foundation recognizes that advances in technology (e.g., quantum computing) mean that even the strongest cryptography may eventually be broken. Therefore, the Sovrin Foundation avoids writing Credentials onto the Sovrin Ledger through a novel technical solution whereby an Issuer creates a Revocation Registry that contains a number called a 'cryptographic accumulator.' The cryptographic accumulator is written to the Sovrin Ledger and is then checked off-chain by a relying party (e.g., a Verifier) when it needs to ensure the validity of a Credential.

Revocation Registries and their cryptographic accumulators use a form of cryptography known as 'zero-knowledge proof' cryptography (ZKP) to prove the validity of a Credential without providing any of the underlying data (Claims) in the Credential (e.g., proving that an Identity Owner is over 21 years of age without disclosing his or her date of birth). Additionally, only the Holders of Credentials can create a Proof of the validity of their Credentials using the Revocation Registry stored on the Sovrin Ledger. Accordingly, a Verifier that needs to know the validity of a Credential can be given a Proof by a Holder, together with the cryptographic accumulator the Issuer placed on the Sovrin Ledger, to determine whether a Credential is still valid and has not been revoked.

When an Issuer needs to revoke a Credential, the Issuer removes the Credential from the dataset used to calculate the cryptographic accumulator off-chain. Once the new dataset is recalculated, the Issuer then posts the numeric value of the new cryptographic accumulator to the Sovrin Ledger. The moment that the cryptographic accumulator value changes on the Sovrin Ledger, the Holder of the Credential will no longer be able to produce a valid Proof of their Credential. Therefore, if a relying party needs Proof that an Identity Holder has a valid driver's license, but the Issuer has removed the Credential from the dataset used to calculate the relevant cryptographic accumulator because the Identity Holder no longer holds a valid driver's license, then the Identity Holder would not be able to produce a Proof of that Credential.

It is unlikely, but possible that the information contained on a Revocation Registry may be considered personal data under the GDPR due to the risk that a cryptographic accumulator may be used as a link to personal data of an identified or identifiable natural person. However, unlike many of the data pseudonymization techniques often associated with blockchain systems (like encryption and hashing), the use of ZKP has novel benefits that may make it superior to other forms of data obfuscation. Given that no regulator has analyzed ZKP, it is uncertain whether the use of ZKP is sufficient for regulators to find the data to be anonymous and therefore not personal data. Accordingly, parties that transact Revocation Registry information may be subject to the GDPR depending on the regulatory treatment of ZKP in the future.

d. Sovrin Ledger Layer Participants - The Sovrin Foundation, Transaction Authors, Stewards, and Transaction Endorsers

Under Permissioned Write Access, there is a low risk that personal data could be stored or transmitted using the Sovrin Ledger for the reasons discussed above. However, to the extent that personal data is written to the Sovrin Ledger (whether inadvertently or in violation of the Sovrin Governance Framework) and until we receive further clarity from EU regulators permitting a more flexible interpretation of the GDPR with respect to DLT, participants in the Sovrin Ledger should consider the following:

i. The Sovrin Foundation

The Sovrin Network is developed through an open community process where the Sovrin Foundation aggregates the collective voice of all volunteer participants. Due to its open nature, the Sovrin Foundation could be removed from its involvement with the Sovrin Network if demanded by the community, for instance, by the community forking the Sovrin Network and assigning a new set of governance rules.

However, based on its current role as the representative body of all Sovrin Identity Owners, the Sovrin Foundation is the principal architect of the Sovrin Network, the custodian of the Sovrin Network codebase, and primarily responsible for the creation of the Sovrin Governance Framework, which is the mechanism by which data processing is directed, dictated, and governed.

The CNIL stated that when a group of entities decide to carry out processing for a common purpose on a blockchain, all entities may be considered joint controllers unless the group of entities has determined which entity will be the controller and which entities will be the processor under the GDPR.[32] The participants concluded that, in its role as the architect of the Sovrin Governance Framework, the Sovrin Foundation is in the best position to fulfill the requirements of the GDPR by serving in this role. Therefore, the Sovrin Foundation and the other participants in the Sovrin Network designated the Sovrin Foundation as the controller of any personal data written to the Sovrin Ledger, consistent with the CNIL's guidance.

Although beyond the scope of this Position Paper, the Sovrin Foundation is developing a GDPR compliance plan that describes methods to respond to data subject access requests and analyzes the lawful basis for processing any personal data written to the Sovrin Ledger, in the event that personal data is written to the Sovrin Ledger and the Sovrin Foundation is the controller of such data.

ii. Transaction Authors

Under Public Write Access, the Sovrin Foundation has determined (after consultation with the community) that when Transaction Authors write their own personal data to the Sovrin Network, that they should also be controllers over that data in the spirit of achieving true self-sovereignty over their data. Therefore, as to a particular Transaction Author's personal data, the Sovrin Foundation and that Transaction Author will be independent co-controllers. In other words, each of the Sovrin Foundation and the Transaction Author independently

determines the purposes and means of processing the Transaction Author's personal data written to the Sovrin Ledger, although it merits highlighting again that the Sovrin Foundation's role vis-a-vis the data is passive and entirely dictated by the Sovrin Governance Framework. This designation of roles and responsibilities is memorialized in a data processing agreement between each Transaction Author and the Sovrin Foundation.

Currently, Transaction Authors must be Trustees or Organizations which are ineligible for the household exemption, as the exemption only applies to natural persons under the GDPR. However, the household exemption may be available in the future if natural persons are permitted to act as Transaction Authors.

iii. Transaction Endorsers

Unlike Transaction Authors, Transaction Endorsers cannot exert control over how transaction data is processed because Transaction Endorsers must endorse every transaction submitted by a Transaction Author (unless such transaction is prohibited by the terms of the Transaction Endorser Agreement). Accordingly, Transaction Endorsers are likely to be processors acting on behalf of Transaction Authors and the Sovrin Foundation, as controllers.

iv. Stewards

By operating a Node on the Sovrin Ledger, Stewards may have some risk of handling personal data in circumstances where Transaction Authors write personal data to the Sovrin Ledger in contravention of the rules and policies of the Sovrin Governance Framework.

To the extent personal data is written to the Sovrin Ledger, Stewards are most likely to be processors because Stewards exercise no control over the transactions or their content and process those transactions only as directed by the Sovrin Governance Framework. It is worth noting that the Sovrin Foundation and Stewards are not joint controllers under Article 26 of the GDPR because the requirements of Article 26 are not satisfied - namely that the Sovrin Foundation and Stewards do not jointly determine the means and purposes of processing. The Stewards simply adhere to the protocol developed by the Sovrin Foundation and set forth in the Sovrin Governance Framework for validating transactions (i.e., processing data) on behalf of the Sovrin Foundation, as the controller.

This designation of roles is supported by the CNIL guidance, which stated that miners (which are a subset of node operators) are not controllers if they only validate transactions, do not participate in the substance of the transactions, and therefore do not define the means and purposes of the processing.[33]

The STOA Report echoed CNIL's interpretation and states, "Miners exercise significant control over the means in choosing which version of the protocol to run. Yet, considering that the criterion of the means has become subsidiary to the 'purposes' criterion, and miners do not determine the purposes of a specific transaction, they unlikely qualify as controllers. This led the CNIL to argue in its 2018 guidance that miners are not controllers. Miners are indeed better seen as 'servants' of the overall system (that benefit financially from its maintenance,

at least in a system that uses proof-of-work). As such, their role has been compared to that of telecommunications providers that are not legally liable for the content of the data they transmit." [34] Miners are akin to Stewards in the Sovrin Network.

To memorialize the role of the Sovrin Foundation as a controller and Stewards as processors under the GDPR, the Sovrin Foundation intends to execute data processing agreements designed to meet the requirements of Article 28 of the GDPR with each Steward. The data processing agreement will be attached to the Sovrin Steward Agreement and will specify the respective roles and responsibilities of the Sovrin Foundation and the Stewards with respect to the processing of personal data on the Sovrin Ledger.

V. Summary of GDPR Roles in the Sovrin Network

The summary of GDPR roles below are applicable to the extent that personal data belonging to a data subject is transmitted using the Sovrin Network at each layer.

Participant	GDPR Role
Credential Exchange Layer	
Issuers	**Data Processors/Data Controllers**
Verifiers	**Data Controllers**
Holders	**Data Controllers**
Agent to Agent Layer	
Developers	**Likely No Obligation** *(with some exceptions)*
Agencies	**Data Processors/Data Controllers** *(depending on scope of activities, either a data processor or data controller)*
Sovrin Ledger Layer	
Sovrin Foundation	**Data Controller**
Transaction Author	**Data Controller**
Stewards	**Data Processor**

VI. Next Steps for the Sovrin Foundation

The Sovrin Foundation will undertake the following policies to support compliance under the GDPR and the protection of personal data (if any) in the Sovrin Network.

a. Enforcing Strict Policies Regarding the Formats and Types of Data Written to the Sovrin Ledger

Under the Permissioned Write Access policies, the Sovrin Foundation will ensure that the Sovrin Governance Framework prescriptively sets forth rules and policies to restrict Transaction Authors from writing personal data to the Sovrin Ledger. Transaction Authors will be advised to use extreme caution when writing information to the Sovrin Ledger, particularly in DID Documents. Transaction Authors will also be educated as to the extremely broad view that the EU regulators take regarding the scope of the GDPR when determining what constitutes personal data. To avoid the risk of human error, the Sovrin Foundation will evaluate the feasibility of imposing technical limitations on the content that may be written to the Sovrin Ledger.

b. Notifying Parties Involved in the Credential Exchange Layer and Agent-to-Agent Layer of Their Obligations Under the GDPR

As detailed above, parties to the Credential Exchange Layer and Agent-to-Agent Layer are likely to have obligations under the GDPR if the elements of the GDPR Applicability Decision-Tree are met and an exemption does not apply. The Sovrin Foundation intends to develop a website (GDPR Portal) with information about the GDPR and its applicability to participants in the Sovrin Network. The GDPR Portal will have information educating participants at the Credential Exchange Layer and Agent-to-Agent Layer that use of the Sovrin Network will not necessarily reduce or otherwise change their obligations under the GDPR, simply because they are now utilizing a self-sovereign identity ecosystem.

c. Providing Participants with Best Practices for GDPR Compliance

The Sovrin Foundation will continue to provide guidance to participants in the Sovrin Network regarding best practices to comply with the GDPR. An example of such guidance (from CNIL) is provided for reference below. Notwithstanding the foregoing, the Sovrin Foundation will make clear that any materials that it provides, including the GDPR Portal, should be used at the participant's own risk and that each participant has a responsibility to ensure that it is fully compliant with the GDPR and any other applicable laws.

The activities detailed below are the CNIL's recommended best practices for achieving GDPR compliance for blockchain platforms.[35]

- *Appointment of a Data Protection Officer (DPO):* Consider whether it is prudent to appoint a DPO, even in the absence of a legal requirement.
- *Prepare a Data Inventory:* Create an auditable data inventory that include a preliminary interview with control team and IT leaders to identify general categories of personal data collection.

  - Create a customized template based on CNIL's recommended format and an IT/Systems questionnaire for general distribution to division heads and senior IT team members identifying data flows relating to the collection, transmittal, and storage of personal data.
  - Review responses to same.
  - Conduct interviews with IT/Cybersecurity teams and key managers that handle personal data who provided responses to questionnaires.
  - Conduct forensic validation of interviews and questionnaires.

- *Prioritize actions:* Based upon the information collected in the Data Inventory, focus on the following critical areas: privacy notices, information regarding vendors regarding their obligations, technical implementation of individuals, security measures, processing of sensitive data, large-scale monitoring activities, evaluation of individual behavior, international transfer considerations, and pseudonymization standards.
- *Conduct data protection impact assessments (DPIA) for any high-risk data activities:* Carry out DPIAs before any new processing that is likely to result in high risks for the rights and freedoms of natural persons.
- *Update the privacy policies, procedures and vendor agreements for compliance:* Prepare internal procedures to manage daily privacy matters, including: privacy team structure, breach response plan, individual rights requests and claims (including exploration of technical solution to support written employee policies), and vendor management (including updating of contracts for onward transfer and other GDPR compliance).
- *Organize records and create governance structures for long term goals:* Develop governance structure to demonstrate compliance with the GDPR through data processing inventory, DPIA records, copies of transfer solutions implemented, notices, consent forms and evidence of consents, procedures for the exercise of individual rights, processor agreements, and breach response implementation.

Bibliography

Sovrin Network Materials

- Sovrin Governance Framework: https://sovrin.org/library/sovrin-governance-framework/
- Sovrin Glossary V2: https://docs.google.com/document/d/1gfIz5TT0cNp2kxGMLFXr19x1uoZsruUe_0glHst2fZ8/edit
- Sovrin: What Goes on the Ledger: Updated September 2018: https://www.evernym.com/wp-content/uploads/2017/07/What-Goes-On-The-Ledger.pdf
- Hyperledger Indy - Indy Walkthrough: https://github.com/hyperledger/indy-sdk/blob/master/docs/getting-started/indy-walkthrough.md
- Hyperledger Indy - Indy - Node - Transactions:https://github.com/hyperledger/indy-node/blob/master/docs/source/transactions.md
- Hyperledger Indy - Indy - Node - Requests: https://github.com/hyperledger/indy-node/blob/master/docs/requests.md
- Is Self-Sovereign Identity the Ultimate GDPR Compliance Tool? (1 of 3, 2 of 3 and 3 of 3): https://medium.com/evernym/is-self-sovereign-identity-ssi-the-ultimate-gdpr-compliance-tool-9d8110752f89
- Sovrin Ledger Access Policies: https://sovrin.org/wp-content/uploads/Sovrin-Ledger-Access-Policies-V2.pdf (See Appendix H of the Sovrin Glossary.)
- Sovrin Network Roles and Permissions, Aries Release: https://docs.google.com/spreadsheets/d/1TWXF7NtBjSOaUIBeIH77SyZnawfo91cJ_ns4TR-wsq4/edit#gid=0
- Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust:https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

[1] This analysis addresses only the GDPR and does not examine the impact of the privacy laws of any other jurisdiction. Capitalized terms not defined in this Position Paper are defined in the Sovrin Glossary or in the GDPR.

[2] There is no single definition of DLT and, like any technology, a distributed ledger can be built in any number of different ways which may result in different analysis. Blockchains are one type of DLT that groups data into "blocks" and "chains" them together chronologically. Nonetheless, the term "blockchain" is commonly used to refer to all DLTs and, in this Position Paper, we will use these terms interchangeably.

[3] For clarity, when we reference "personal data" in this Position Paper, we are referring to personal data of EU data subjects for the purposes of our GDPR analysis.

[4] These layers are summarized in Appendix D of the Sovrin Glossary, and details of the roles of each layer are covered in Appendices E, F, G, and H.

[5] Although not described as its own layer in this paper, the Sovrin Network also includes a Governance Framework Layer that consists of written principles, policies, terminologies and standards to address the specific needs of various Sovrin Network participants.

[6] The term "Identity Owner" is not used to imply legal ownership of personal data in a property sense. Instead it refers to the ability to independently prove a self-sovereign identity using digital credentials from a digital wallet.

[7] Also called a "Peer DID" (DID stands for "Decentralized Identifier"). See the Peer DID Method Specification: https://openssi.github.io/peer-did-method-spec/ (last visited Dec. 3, 2019).

[8] Anywise DIDs are sometimes informally called Public DIDs because they are typically written to a public ledger such as the Sovrin Ledger.

[9] Agents are not participants in the Agent-to-Agent Layer because they are simply software and not entities or natural persons.

[10] Nodes are not participants in the Sovrin Ledger Layer because they are software and not entities or natural persons.

[11] GDPR, Art. 3.

[12] GDPR, Art. 4.

[13] GDPR, Recital 26.

[14] Blockchain and the GDPR, European Union Blockchain Observatory and Forum, at 11 (Oct. 16, 2018) ("EU Blockchain Observatory Report"), https://www.eublockchainforum.eu/reports.

[15] Solutions for a responsible use of the blockchain in the context of personal data, CNIL, https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf (last visited Jan. 3, 2019).

[16] Resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation, European Parliament, (Oct. 3, 2018), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0373+0+DOC+XML+V0//EN&language=EN.

[17] Blockchain and the General Data Protection Regulation, STOA, (Jul. 2019), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

[18] Martha Bennett, et al., Don't Let GDPR Derail Your Blockchain Strategy - Distributed Ledger Technology Can Even Become Part of GDPR Compliance Frameworks, 2-3 (Dec. 21, 2018).

[19] Michéle Finck, Blockchains and Data Protection in the European Union 16-18 (Max Planck Inst. for Innovation & Competition Research, Paper No. 18-01, Nov. 30, 2017).

[20] EU Blockchain Observatory Report, at 16.

[21] Art. 29 WP Opinion 05/2014 "Anonymization Techniques" (0829/14/EN, WP 216), at 20-21.

[22] GDPR, Recital 29.

[23] Breyer v. Bundesrepublik Deutschland (2016) Case C-582/14.

[24] See supra note 20.

[25] GDPR, Recital 29.

[26] Id.

[27] František Ryneš v. Úřad pro ochranu osobních údajů (2014) Case C-212/13; GDPR, Recital 18.

[28] See supra note 14.

[29] See supra note 16 at 11-12.

[30] See supra note 14 at 2.

[31] Id.

[32] Id.

[33] Id.

[34] Blockchain and the General Data Protection Regulation, STOA, (Jul. 2019), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

[35] General Data Protection Regulation Guide for Processors, CNIL (Sept. 2017), https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil_en.pdf.

sovrin
identity for all

Sovrin Foundation

86 N University Ave.
Suite 110
Provo, UT 84601

+1 801 701-1848

Info@Sovrin.org