iOwn.Me Privacy Policy

1. Introduction

At iOwn.Me, your privacy is paramount. We are committed to safeguarding your data while providing you with the utmost in privacy and data protection services. This Privacy Policy outlines our practices in collecting, using, and protecting your information, particularly within our patented Community of Trust, the Declaration Certificate (Dec Cert) and ADDIV system.

2. Information We Collect

- **Personal Information:**

  Includes but isn't limited to your name, email address, postal address, phone number, and other identifiable details. This is your data as defined in the CoT Agreements.

- **Non-Personal Information:**

  Data that doesn't directly identify you, like browsing history, device type, and location data may be collected in the future but it is your data.

3. How We Use Your Information

Your information aids us in:

- Enhancing our services, including the CoT, ADDIV, and Dec Cert system.
- Communicating with you regarding service updates, offers, and news.
- Responding to your queries, feedback, or complaints.
- Ensuring a cohesive community experience.

4. User Rights

Rights to Your Information:

- **Right to Know:** Request details about the personal information we collect, use, or share.
- **Right to Access:** Gain access to the personal information we hold about you.
- **Right to Request Deletion:** Ask for the removal of your personal data from our records.
- **Right to Correct:** Update or correct inaccuracies in your personal data.
- **Right to Object:** Challenge the collection or processing of your data under certain circumstances.

5. Data Protection and Sharing

The Community of Trust (CoT):

- At the core of the "iOwn.Me" ecosystem is the Community of Trust (CoT), a legally defined entity that establishes a secure environment for individuals to manage their

digital identities. The CoT operates under a robust legal framework that outlines cybersecurity standards, privacy rules, and governance structures. This framework ensures that participants' rights and personal information are protected within the laws of the relevant jurisdiction.

The CoT serves as a foundation for individuals to assert their digital self-ownership. By joining a CoT, individuals agree to abide by the established rules and standards, creating a collective commitment to data privacy and security. This collective strength reinforces the individual's claim to their digital identity, making it harder to challenge or dismiss.

The Declaration Certificate:

- Within the CoT**,** individuals can obtain a Declaration Certificate, a formal document that serves as a tangible assertion of their digital self-ownership. The certificate follows a standardized methodology, ensuring a consistent application of the "iOwn.Me" principle across all participants.
- The Declaration Certificate is more than just a symbolic gesture. It leverages a repeatable process to timestamp the individual's declaration, creating an auditable record that can be used as evidence in legal proceedings. By linking the certificate to the CoT framework, the individual's claim is structured and recognized, deriving its strength from the community's collective agreement.

The Network Privacy Patent:

- The "iOwn.Me" concept is underpinned by a comprehensive patent (US 10,084,757) that grants individuals unequivocal legal ownership and rights to all data pertaining to themselves, whether knowingly or unknowingly transmitted across any network. This patent is a crucial component of the CoT framework, providing a legal foundation for the individual's claim to their digital identity.
- The patent validates the "iOwn.Me" process, confirming its uniqueness and innovation. By establishing data ownership as a fundamental property right, rather than just a privacy concern, the patent elevates the significance of the individual's declaration. It also provides legal protection against infringement, safeguarding the integrity of the "iOwn.Me" declaration when combined with the CoT's methodology.

The Distributed Digital Identity Vault System (ADDIV):

- To support the practical implementation of digital self-ownership, the "iOwn.Me" ecosystem includes a Distributed Digital Identity Vault System. This system serves as a secure repository for individuals to store and manage their personal data within the CoT.
- The Identity Vault is overseen by a Privacy Authority, responsible for monitoring and regulating data usage within the CoT. Individuals have the power to set their data preferences, including sharing and monetization options, in accordance with their specific needs and the legal requirements of their jurisdiction.
- By providing individuals with a centralized "Dashboard" to control their data, the Identity Vault System empowers them to manage their digital footprint effectively. This not only enhances privacy but also opens up new opportunities for individuals to monetize their data on their own terms.

Data sharing between CoTs:

- **iOwn.Me Community of Trust (CoT) Interconnection Agreement Overview**

  The iOwn.Me Community of Trust (CoT) Interconnection Agreement outlines the framework for the secure and private interconnection of multiple CoTs. This agreement, incorporating elements from the Master CoT Owner Agreement, the Interconnection Security Agreement, and the Purpose Specific Information Sharing Agreement, details the responsibilities, legal framework, and operational standards required for CoT Owners and Interconnected Parties.

- **Scope**

  This agreement sets forth the terms and conditions applicable to interconnection-related services between CoT Owners and Interconnected Parties. It incorporates relevant work orders and ancillary documents that define specific services and interconnection details.

- **Purpose**

  The primary purpose is to establish secure interconnections between CoTs, allowing for the exchange and management of digital identities and associated data while adhering to strict privacy and security standards. The agreement includes the necessary tools and technologies to support the deployment and operation of CoTs.

- **Term and Termination**

  The agreement takes effect on the execution date and continues for one year, with automatic renewals unless terminated. Termination can occur with written notice for breaches or if the operation of the CoT becomes unlawful.

- **Work Orders**

  Specific interconnection services and responsibilities are detailed in work orders executed by the parties. These work orders are governed by the terms of the master agreement.

- **Intellectual Property (IP)**

  Each party retains ownership of its IP. Limited licenses may be granted for specific purposes as outlined in the agreement and work orders. IP rights related to iOwn.Me services are subject to separate licensing terms.

- **Confidential and Proprietary Information**

  Both parties must protect confidential information, using it only for the performance of the agreement and ensuring it is not disclosed to unauthorized parties. Confidential information includes non-public technology, legal frameworks, and other sensitive data.

- **Responsibilities of the Parties**
    - **Data Sharing:** The parties agree to protect and share data as specified in ancillary agreements, following defined data protection and privacy standards.
    - **Security:** Each party must meet minimum cybersecurity standards, including adherence to the NIST Cybersecurity Framework and other relevant regulations. Regular security reviews and certifications are required.
    - **Privacy:** Parties must comply with minimum privacy standards, ensuring user data is protected and shared only with explicit consent. GDPR and other international privacy laws are followed.
    - **Cyber Insurance Policies:** Each party must maintain cybersecurity insurance covering their CoT and interconnections, ensuring coverage for professional liability, privacy, and cyber-risk.
- **Interconnection Security**

  The interconnection security agreement outlines the technical and security requirements for connecting CoTs. This includes encryption standards, incident reporting protocols, and trusted behavior expectations. The agreement also details audit responsibilities, user community guidelines, and specific equipment restrictions.

- **Cooperation and Communication**

  Parties agree to cooperate in implementing the security policies, meeting regularly to ensure compliance. Communication regarding the CoT and services is conducted electronically using licensed software and protocols.

- **Remuneration and Fees**

  Fees for services are outlined in work orders, with monthly invoicing and payment terms specified. Parties are responsible for their respective fees and taxes.

- **Dispute Resolution**

  Any disputes arising from the agreement are first submitted to non-binding mediation, followed by binding arbitration if necessary. The agreement specifies the governing law and venue for legal actions.

- **Amendments and Modifications**

  Any changes to the agreement must be in writing and mutually agreed upon by the parties. Unauthorized assignments or transfers are void.

- **Interconnection Between CoTs**

  The interconnection of CoTs allows for the seamless sharing of digital identity data across multiple trusted networks. This is achieved through:

  - **Mutual Adherence to Standards:** Both CoT Owners and Interconnected Parties must adhere to agreed-upon cybersecurity and privacy standards.
  - **Use of Secure Technologies:** Interconnections utilize secure technologies such as encryption, firewalls, and intrusion detection systems to protect data in transit and at rest.
  - **Data Sharing Agreements:** Detailed agreements specify the type of data shared, the purpose of sharing, and how the data will be protected.
  - **Regular Audits and Reviews:** Continuous monitoring and regular audits ensure compliance with security and privacy standards.
  - **Incident Reporting and Management:** Clear protocols for incident reporting and management help quickly address any security breaches or privacy violations.

  By establishing these secure interconnections, CoT Owners can offer robust digital identity management services, ensuring the privacy and security of user data while enabling interoperability and trust among different CoTs.

6. Opt-Out & Communication Preferences

You have the choice to opt out of our communication list. You can also mute notifications or unsubscribe from newsletters via profile settings or by reaching out to us.

7. International Users

Our commitment extends globally. We respect international data protection laws, offering extended rights to users from regions like the EU (General Data Protection Regulation) and Canada.

8. Changes to Privacy Policy

While we may update this Privacy Policy, major changes will be communicated. Your continued interaction signifies consent to any changes.

9. Governing Law

This Privacy Policy is under the jurisdiction of Texas law, USA. By providing us with information, you consent to the application of this law.

10. Contact Us

For queries, clarifications, or feedback related to this Privacy Policy, please contact us. Your trust and privacy are of utmost importance to us at iOwn.Me. By engaging with our services, you agree to the terms outlined in this Privacy Policy.