Privacy Policy: SovCore B.V.

Document Ref: SC-PP-2026-01 Effective Date: April 1, 2026

At SovCore B.V. ("SovCore"), privacy is not a policy—it is our core architecture. This document explains how we handle personal data under the **General Data Protection Regulation (GDPR)** and **NEN 7510** standards.

1. The "Zero-Knowledge" Difference

SovCore is a Zero-Knowledge service provider. This means:

- **We cannot see your data:** All encryption happens in your browser. We store only encrypted fragments (ciphertext) that are mathematically indecipherable to us.
- **We do not track your content:** We have no technical means to index, search, or profile the files you store in your vault.

2. Roles and Responsibilities (GDPR Art. 28)

- **The User as Data Controller:** You (or your organization) are the Data Controller for any personal, medical, or legal data you upload to the vault. You retain full control over who has access.
- **SovCore as Data Processor:** SovCore acts as the Data Processor. Our processing is limited to the automated storage and retrieval of encrypted fragments as directed by your authenticated session.

3. Data We Collect

We adhere to the principle of "Data Minimization." We only collect:

- **Account Metadata:** Name and professional email address.
- **Authentication Data:** Public identifiers from your **EUDI Wallet** or **SD-JWT** (we never see your private keys).
- **Analytical Data (Privacy-First):** To improve our website, we use **Simple Analytics**. This is a privacy-first tool hosted in the Netherlands that does not use cookies, does not collect personal data, and does not track you across other websites. We receive only aggregated, anonymous insights.

4. Data Storage and Sovereignty

- **Infrastructure:** Our marketing site is hosted on **OVHcloud (France/EU)**, and our vault infrastructure resides on **Scaleway (Netherlands/EU)**.

- **No International Transfers:** SovCore does not transfer your data to third countries (e.g., the United States). Our architecture ensures that even if a foreign entity attempted to access the infrastructure, the data would remain unusable ciphertext.

5. Technical and Organizational Security

We implement state-of-the-art measures to protect the platform:

- **WASM Isolation:** Sensitive cryptographic operations are sandboxed away from the browser's JavaScript environment.
- **Cross-Origin Isolation (COI):** OS-level process isolation to prevent side-channel attacks.
- **Integrity Checks:** Every data fragment is verified using SHA-256 hashes via the Origin Private File System (OPFS).

6. Your Rights under GDPR

You have the right to access, rectify, or delete your account data.

- **Note on Erasure:** Deleting your account will permanently destroy your encrypted fragments.
- **Note on Portability:** Because we do not hold your keys, we cannot "export" data on your behalf if you lose access to your EUDI Wallet credentials.

7. Authorized Sub-Processors

We engage a limited number of sub-processors to provide our service. All are bound by strict Data Processing Agreements (DPAs):

- **OVHcloud (EU):** Web hosting for marketing.
- **Scaleway (EU):** Encrypted object storage and compute.
- **Simple Analytics (NL):** Privacy-first website telemetry.

8. Contact Information

For questions regarding your privacy or to exercise your GDPR rights:

SovCore B.V. – Data Protection Officer Email: dpo@sovcore.eu

Zoetermeer, The Netherlands

Chidinma Egbukichi

Digitally signed by Chidinma Egbukichi
Reason: I am approving this document
Date: 2026.03.31 16:42:38 +02'00'