Privacy Statement

Privacy Statement for omnichain.ca. Published 2026-10-25. Download this statement (PDF).

What this site collects

Omnichain (omnichain.ca) collects the minimum needed to operate the mining platform:

- **WordPress account data** if you register an account: your username, email address, and profile details you provide.
- **Wallet addresses** you connect to the site. A wallet address is public on-chain data — anyone can view an address's transactions on the public Avalanche ledger — and it is not private information. The site verifies ownership by message signature.
- **Uploaded documents** (bills and receipts you choose to upload for mining), their extracted data (vendor, amount, tax), their SHA-256 hashes, and the resulting allocation and payout records.
- **Server logs** (IP address, browser type, pages requested, timestamps) generated by the hosting infrastructure, and **cookies** used for sign-in sessions and site preferences.

What the site never collects

The site never sees, asks for, stores, or transmits your wallet's **private key** or **Secret Recovery Phrase**. Wallet verification is by cryptographic signature only. Anyone who asks for your recovery phrase in connection with this site is not us — do not share it, ever.

How uploaded documents are processed

- **OCR processing.** Uploaded documents are processed by a third-party OCR service (OCR.space) to extract the vendor, amount, and tax figures. The document image is transmitted to that service for processing as part of the mining pipeline.
- **Hash-only anchoring.** The stored copy of your document is hashed with SHA-256, and the hash only is anchored in a transaction on the Avalanche blockchain as a public proof of processing. The document itself is never placed on a blockchain and cannot be reconstructed from its hash.
- **Vault storage.** Stored documents are kept in an access-controlled vault on the server; the vault directory refuses all direct web access and file names are randomized.
- **Gated serving.** Your stored documents are served only to you, only through a checked endpoint that re-verifies your wallet signature session, the document's ownership, and the dashboard memory gate — a live hold of at least 5 OMC — at the moment of each request. There are no direct or shareable file URLs.

What is public by design

Blockchain records are public: document hash anchors, token transfers (including mining payouts from the treasury), and wallet addresses can be viewed by anyone on a block explorer such as snowtrace.io. This transparency is a design feature of the platform — it is how payouts and anchors can be verified — and it cannot be switched off for on-chain activity.

Sharing and sale of information

We do not sell personal information. Information is shared only with the service providers needed to operate the platform: the hosting provider (Web Hosting Canada), the OCR processor (OCR.space, for uploaded documents), and the public Avalanche network (hashes and transactions, as described above).

Retention and your choices

Uploaded documents and account records are retained while your participation is active, so that your dashboard history and document memory remain available to you. On-chain records (hash anchors and transfers) are permanent by the nature of blockchain technology and cannot be deleted. For off-chain records, you may request access to, correction of, or deletion of your personal information by contacting the site administrator at admin@omnichain.ca. Deleting stored documents ends the associated dashboard memory access for those documents.

Legal framing

This statement is framed under Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). By using the site, you consent to the processing described here, including OCR processing of documents you upload and the public anchoring of document hashes. We may update this statement as the platform evolves; material changes will be published on this page with a revised date. Questions about privacy on this site: admin@omnichain.ca.