goodfinity

Goodfinity Sovereign Data Privacy Policy

Last modified: October 29, 2026

Goodfinity Sovereign Data Configuration. This policy applies only to clients whose Order Form, Statement of Work or Sovereign Data Rider designates the Sovereign Data Configuration. Everyone else, including every visitor to goodfinity.ca, is covered by the Goodfinity Privacy Policy at goodfinity.ca/privacy-policy.

A note before the legal language

The Sovereign Data Configuration exists because First Nations have told Canadian governments and software vendors the same thing for decades: our data is not yours. That principle, formalized in the OCAP® framework (Ownership, Control, Access, Possession) developed by the First Nations Information Governance Centre, is the design brief for this configuration. OCAP® is a registered trademark of the First Nations Information Governance Centre; Goodfinity's Sovereign Data Configuration is built to the principles and is not certified by, affiliated with, or endorsed by the Centre.

If anything in this policy is unclear, contradicts what we told you in a sales conversation, or appears to give us more rights over your community's data than you expect, tell us and we will fix the document. If this policy and your signed agreement ever conflict on the handling of your data, whichever gives your community more control applies.

1. Who we are and who this policy covers

Goodfinity is a trade name of Level Up Strategies Inc., a British Columbia corporation based in Kelowna ("Goodfinity," "we," "us").

This policy covers one thing: clients on the Sovereign Data Configuration, meaning First Nations, tribal councils, Indigenous organizations, and any other client whose agreement designates it. It is written for you. Your Customer Agreement, including any Sovereign Data Rider, controls over this policy if the two conflict, except where this policy gives your community more control.

Visitors to goodfinity.ca, including the pages that describe the Sovereign Data Configuration, and clients on the Standard Data Configuration are covered by the Goodfinity Privacy Policy at goodfinity.ca/privacy-policy, not by this one. Reading this policy, or asking about it, does not bring anyone under it.

2. Applicability

This policy applies to a deployment only when the client's Order Form, Statement of Work, or Sovereign Data Rider designates the Sovereign Data Configuration. The configuration is provisioned as a dedicated deployment with its own governance profile, and the commitments below are enforced by that deployment, not by request. A client on the Standard Data Configuration cannot invoke this policy; it can contract for the Sovereign Data Configuration, at which point its data is migrated and this policy applies from the migration date.

3. The OCAP® commitments

- **Ownership.** Your community owns its data and every report produced from it. We are a processor acting on your instructions.
- **Control.** Your community's designated governance authority defines consent policies, disclosure rules, and approval workflows in the platform. The platform enforces them: an operation with no recorded consent is denied, not allowed by default. Consent can be withdrawn at any time with immediate effect.
- **Access.** Every action on your data, including every AI inference, export, external transmission, and key use, is written to an append-only audit log your governance authority can read at any time and export in machine-readable form, without giving a reason.
- **Possession.** Your data is held on infrastructure in Canada under an encryption key dedicated to your deployment, AI processing stays on Goodfinity's own hardware in Kelowna, British Columbia, and on request the deployment runs on infrastructure you control, where the keys are yours.

4. What we process

Whatever your community uploads or connects: funding agreements and reporting templates (Indigenous Services Canada, CMHC, PHAC, provincial funders), program and service records, financial records, member or client records from your administration systems, reports drafted by your staff or generated by the platform, and the approvals routed through the governance workflow. The scope is set by your agreement and the sources you choose to connect.

5. Data residency and isolation

- Your data is stored only in Canada and, except for AI processing you have consented to under Section 6, processed only in Canada, in a dedicated single-tenant deployment: its own database and application instances, separate from every other client. Your Statement of Work chooses where that deployment runs: on Amazon Web Services in the Canada (Central) region, or on dedicated hardware Goodfinity operates in Kelowna, British Columbia. On request, and as agreed in your Statement of Work, it can instead run on infrastructure your community controls.

- Encryption at rest, on the AWS placement, uses a key created for your deployment and used for nothing else (an AWS Key Management Service key, administered by Goodfinity in its own AWS account under a rule that never deletes the key while any recoverable copy of your data exists). On the Kelowna placement, your deployment's database and files sit on an encrypted volume that the platform verifies before it will start, and every file is additionally encrypted by the application before it is written to disk. In every placement, designated personal-information fields are additionally encrypted at the application layer with a key generated for your deployment. Access to decrypted data is limited to the platform processes that need it and is logged. Where your Statement of Work places the deployment on infrastructure your community controls, the keys are held by you.
- Encryption in transit requires TLS 1.2 or higher.
- Backups inherit the same encryption and stay inside your deployment in Canada, on whichever placement you choose. Automated database backups are taken daily and kept for seven (7) days. No backup copy leaves your deployment unless your governance authority has recorded consent for an offsite copy.
- Nothing in the processing pipeline sends your data outside Canada unless your governance authority has recorded consent for a specific provider (Section 6).

6. Artificial intelligence

The platform uses AI to draft compliance narratives, analyse documents, and answer questions about your data. On the Sovereign Data Configuration, AI processing runs on open-source models hosted on Goodfinity's own hardware in Kelowna, British Columbia. Your data does not leave that hardware for AI processing and is not sent to any AI provider. Every output passes through automated checks (that figures trace to your records, that withheld names do not appear, that nothing was silently dropped) before anyone sees it. No AI request is made until your governance authority has recorded a consent policy that covers it; a request with no recorded consent is refused, and the refusal is logged.

- **Kelowna-hosted models (default).** Open-source models, currently from the Qwen family, running on Goodfinity-owned hardware in Kelowna. Narrative quality is lower than the cloud option and we say so plainly. We name the models in use on request and tell your governance authority in writing before we change them.
- **Cloud model, only on recorded consent.** If your governance authority prefers higher narrative quality and records consent for it, AI requests may instead be sent to Anthropic, PBC (Claude API), a United States company, under commercial terms that prohibit training on your data and delete inputs and outputs within thirty (30) days. Consent can be withdrawn at any time, and the deployment returns to the Kelowna-hosted models.

Under either option: we never use your data to train, fine-tune, or improve any model; AI output is a draft that your designated staff review before anything is submitted to a funder or regulator; and AI does not speak for your community.

7. No secondary use
We do not use your data for any purpose other than performing the services for you. We do not aggregate or combine your data with the data of any other client or community, in de-identified form or otherwise. We do not benchmark, do not build products from your data, and do not train models on it. Internal product metrics use only counts and metadata that contain no community data. Any exception requires your governance authority's separate written consent, which can be withdrawn at any time.

8. Who else touches your data
AI processing happens on our own hardware in Kelowna (Section 6) and involves no third party unless your governance authority chooses the cloud option. The third parties are:

- **Amazon Web Services, Canada (Central) region**: hosting, compute, storage, and key management for your dedicated deployment, where your Statement of Work places it on AWS. On the Kelowna placement, hosting involves no third party.
- **Anthropic, PBC (United States)**: AI processing, only if your governance authority has chosen the cloud option and recorded consent (Section 6).
- **Cloudflare**: secure network tunnel and DNS in front of the platform; traffic in transit only. Cloudflare does not retain request logs by default and stores none of your content.
- **Google Workspace:** support correspondence only, held in Google's data centres, which may be outside Canada. Production data is never sent by email.
- **Wix**: the public website only; no client data.

We will tell your governance authority in writing at least thirty (30) days before adding or replacing a provider that would process your data, and your community may object and, if we cannot resolve the objection, end the affected services without penalty.

9. Disclosure only as you direct
We will not transmit your data or any report to a funder, regulator, or any other external party except as directed by your designated governance authority through the platform's approval workflow or in writing. If a court or authority compels disclosure, we will tell you before complying unless the law prohibits it, and we will disclose only what is required.

10. Your community's rights
Exercisable at any time, without penalty and without giving a reason:

- **Export.** A complete export of all data provided to or generated within the platform, in open formats (CSV, JSON, PDF, and source documents in their original form), within thirty (30) days of request.
- **Correct.** Correction of any inaccurate data through the platform or through support.
- **Govern.** Define, change, or revoke consent policies, disclosure rules, and approval workflows at any time; changes take effect immediately and are versioned.
- **Audit.** Read and export the audit log at any time.
- **Know.** Ask how any record was handled, who accessed it, or how the platform processed it; we answer within ten (10) business days.

- **Leave.** End the service at any time. We provide the export within thirty (30) days. We then take one final encrypted snapshot so that nothing is lost while you verify the export, delete the production deployment within thirty (30) days after the export window closes, let the automated backups expire within their seven (7) day retention period, and destroy the final snapshot and schedule the encryption key for deletion once your governance authority confirms the export is complete. We deliver written confirmation of each step. The audit log is retained for seven (7) years for your community's own forensic needs unless you ask for earlier deletion.

11. Personal information about individuals

For data about identifiable individuals, such as community members, employees, and service recipients, your community is the organization accountable under PIPEDA and any applicable provincial or health-information legislation, and your community's own laws and customs. Individuals exercise access, correction, and withdrawal rights through your community's administrator; consent policies can be withdrawn at any time with immediate effect, individual records can be corrected or deleted on your administrator's instruction, and we provide the technical means to respond. For questions about our own practices, see Section 15.

12. If something goes wrong

If we become aware of unauthorized access to or disclosure of your data, we will contain it and preserve evidence; notify your designated governance contact within seventy-two (72) hours of confirming the incident, on any day of the week; provide a written report of what happened, what was affected, what we did, and what we recommend; cooperate with your community's investigation; and make any regulatory notifications the law requires. We keep a record of every incident for at least twenty-four (24) months.

13. Retention

During the term, your data is kept for as long as your agreement is in force plus the time needed to complete any reporting in progress. After the term, Section 10 applies. Once your governance authority confirms the export, we keep no copy.

14. Compliance program

Our security and privacy program is being built toward SOC 2 Type II and the Canadian Centre for Cyber Security's cloud service provider assessment, with controls crosswalked to ITSG-33, on infrastructure (Amazon Web Services, Canada regions) that the Cyber Centre has assessed at its Cloud Medium level, the profile formerly called Protected B, Medium Integrity, Medium Availability. That assessment is the provider's, not ours. We do not hold a SOC 2 report or a Cyber Centre assessment today, and we will not claim one until we do. Communities that need specific assurances for their funders or auditors should raise them during onboarding.

15. Contact and complaints

Privacy Officer: Brandon Farr, founder. Email privacy@goodfinity.ca. Mail: Privacy Officer, Level Up Strategies Inc. dba Goodfinity, 101 – 1865 Dilworth Drive, Kelowna, British Columbia, Canada, V1Y 9T1.

Disputes that concern your data or these commitments go first to a meeting that includes your designated governance authority, conducted in a manner consistent with your community's own practices, before any other step. You may also complain to the Office of the Privacy Commissioner of Canada or the Office of the Information and Privacy Commissioner for British Columbia.

16. Changes

We will give clients on the Sovereign Data Configuration at least thirty (30) days' written notice of any material change to this policy, and a change log on request. A change never reduces the commitments in your signed agreement.