goodfinity

Goodfinity Standard Privacy Policy

Last modified: October 29, 2026

1. About This Policy

Goodfinity, a division of Level Up Strategies Inc. ("Goodfinity," "we," "us," or "our"), is a Canadian software and data services company offering impact reporting and donor analytics to charities and nonprofits. This Privacy Policy describes how we collect, use, disclose, and protect personal information about:

- visitors to our websites, goodfinity.ca and goodfinity.com (the "Sites");
- people who contact us, request a demonstration, or sign up for our mailing lists;
- staff and administrators of client organizations who hold accounts on the Goodfinity Insights Engine (the "Platform"); and
- people we connect with for business development and partnerships.

Client data is governed by a separate agreement. When a client organization uploads documents to the Platform, connects an external data source, or sends us records as part of a consulting engagement, the personal information in those records about the client's donors, volunteers, staff, and constituents is "Client Data." We process Client Data only on the client's instructions under our Data Processing Agreement or Master Services Agreement. For that data the client, not Goodfinity, is the organization accountable under privacy law, and the client is responsible for notifying the individuals concerned. Sections 5, 7 and 8 of this Policy explain our practices for Client Data in plain terms; the agreement governs the details.

Two data configurations. Goodfinity offers two configurations of the Platform. This Policy describes the Standard Data Configuration, which applies to every client unless its Order Form or Statement of Work designates the Sovereign Data Configuration. The Sovereign Data Configuration carries additional commitments described in the Sovereign Data Privacy Policy, published at goodfinity.ca/sovereign-data-privacy, which applies only to a designated deployment. Section 16 explains the difference and how a client obtains it. A client cannot elect the Sovereign Data Configuration by request after signing; it is a contracted configuration.

2. Information we collect

- Identifiers and contact information you provide: name, email address, phone number, organization name, job title.
- Commercial information about your organization: size, type of nonprofit, services of interest.
- Internet activity on the Sites: IP address, browser and device information, pages viewed, referring URL, approximate location derived from IP.
- Correspondence: the content of your emails, support tickets, and meeting notes with our team.
- Marketing preferences: mailing-list subscriptions, communication preferences, event attendance.
- Platform account and authentication information: name, work email, organization, assigned role, and a hashed password. We never store passwords in plain text.
- Platform usage and technical logs: actions taken in the Platform, request logs, IP address, timestamps, and request identifiers used for security and troubleshooting.
- Billing and contact information associated with a client account. Payment card details for subscriptions purchased through our website are collected and processed by our checkout provider under its own terms; Goodfinity does not receive or store full card numbers.

We do not intentionally collect sensitive personal information through the Sites or Platform accounts, and we do not collect precise geolocation.

3. Where this information comes from

- Directly from you, when you fill out a form, contact us, subscribe, or create or use an account.
- Automatically, through cookies and similar technologies when you use the Sites. The Sites run on Wix, which sets cookies that are strictly necessary to operate the Sites and, depending on the features we have enabled, analytics and marketing cookies that tell us how visitors found and used the Sites. You can block or delete cookies in your browser settings, and the Sites still work without the non-essential ones. The Platform itself uses only the browser storage strictly necessary to keep you signed in and to operate securely; it uses no advertising or third-party tracking cookies and no web analytics.
- From publicly available sources, such as charity registries and professional directories, when we research prospective clients.
- From the service providers we use to run our business, such as our customer-relationship and email systems.

4. How we use personal information

We use personal information to operate, maintain, secure, and improve the Sites and the Platform; to respond to inquiries, deliver demonstrations, and onboard clients; to send service communications, product updates, and marketing emails you can unsubscribe from at any time; to understand how the Sites and Platform are used; to protect our clients and our business from fraud, abuse, and security threats; to comply with law, including tax and accounting obligations; and to pursue our legitimate business interests, including business development, partnerships, and reporting to our investors and lenders.

When we demonstrate the Platform to prospective clients we use synthetic sample data, not the personal information of real donors or staff. We use a client's data only to provide that client with insight into its own organization. We never use one client's data to benefit another client.

We do not use personal information for automated decision-making that produces legal or similarly significant effects about you.

5. Artificial intelligence

The Platform uses artificial-intelligence tools to analyse documents, answer questions, and draft report content. Today our AI provider is Anthropic, PBC (the Claude API), a United States company whose processing takes place outside Canada. The text and document context sent for analysis may contain personal information from Client Data.

Our commitments:

- We never use Client Data, or any personal information, to train, fine-tune, or improve an AI model, ours or anyone else's.
- We engage only AI providers whose terms prohibit the use of our data to train their models. Anthropic's commercial terms do this, and Anthropic deletes API inputs and outputs from its systems within thirty (30) days of receipt unless content is flagged for a usage-policy violation or the law requires longer.
- AI output is a draft. Our team or the client reviews it before it is relied on.
- We do not make automated decisions about individuals.

Clients that need AI processing kept on Goodfinity's own hardware in Canada, and made only on their governance authority's recorded consent, can contract for the Sovereign Data Configuration (Section 16).

6. How we share personal information

- **Service providers** that help us run the Sites, the Platform, and our business: cloud hosting and storage, artificial-intelligence processing, email and marketing platforms, customer-relationship management, customer support, accounting, and payment processing. Each is bound by contract to protect your information and to use it only to provide services to us. The providers that process Client Data are listed in our Third-Party Providers list, available on request, and clients are told when that list changes in a way that matters.
- **Professional advisors**, including lawyers, accountants, and auditors.
- **Government authorities and other third parties**, where required by law or legal process, or to protect our rights.
- **A prospective or actual purchaser** of our business, in the event of a corporate transaction, under confidentiality obligations.]

We do not sell personal information. We do not use advertising networks or data brokers in connection with the Platform. We do not share personal information for cross-context behavioural advertising as those terms are defined in United States state privacy laws. If any of this ever changes, we will update this Policy and provide the opt-out mechanisms the law requires.

7. Connected services

A client can connect an external data source to the Platform, such as QuickBooks Online, Google Drive, Microsoft OneDrive or SharePoint, or a supported donor database, so that its own records can be imported for analysis and reporting. These connections are off by default; nothing is accessed until an authorized user at the client enables and authorizes the connection.

- **Authorization.** Each connection uses the provider's own sign-in and authorization flow. Goodfinity never sees or stores the user's password for the provider. Access tokens are stored encrypted and used only for that client's connection.
- **What we access.** Read-only access to the records the client chooses to import. We do not write to, modify, or delete anything in the connected service.
- **Why.** Solely to provide the services the client has asked for. We do not use connected-service data for advertising, we do not sell it, and we do not use it to train AI models.
- **Disconnecting.** An authorized user can disconnect at any time from the Platform or from the provider's own account settings. We then stop accessing the source and revoke the stored credentials.

- **Google API Services.** Goodfinity's use and transfer of information received from Google APIs to any other app adheres to the Google API Services User Data Policy and the Google Workspace API User Data and Developer Policy, including their Limited Use requirements. Data obtained from Google Drive is used only to provide or improve the features the user has requested, is not sold, is not used or transferred for advertising or any unrelated purpose, is not used to develop, improve, or train generalized AI or machine-learning models, and is accessed by humans only with the user's affirmative consent, where required for security or to comply with law, or where it has been aggregated and de-identified.
- **Your relationship with the provider.** Your use of QuickBooks Online, Google Drive, Microsoft OneDrive or SharePoint, or any other connected service is also governed by that provider's own terms and privacy policy.

8. Where we store and process information

Goodfinity is headquartered in British Columbia, Canada. The Platform, including its database, application services, and uploaded-document storage, is hosted with Amazon Web Services in Canada, so Client Data and Platform account information are stored and processed at rest in Canada. Network traffic to and from the Platform passes through Cloudflare's edge network in transit.

Some processing occurs outside Canada: AI processing by Anthropic, a United States company; email through Google Workspace, which offers no Canadian data region, so mail is held in Google's data centres and may be outside Canada; and marketing email through our email-marketing platform in the United States. Information processed outside your home jurisdiction is subject to the laws of the jurisdiction where it is processed, which may include lawful-access requests from that jurisdiction's authorities. We use contractual, technical, and organizational safeguards so that information receives a comparable level of protection wherever it is processed. If you are a resident of Quebec and have questions about the transfer of your personal information outside Quebec, contact our Privacy Officer (Section 17).

9. How long we keep information

We keep personal information only as long as needed for the purposes in this Policy or as required by law:

- marketing-list data: until you unsubscribe, after which we keep your email address only on our suppression list so we honour your request;
- correspondence and contact records: for as long as our relationship with your organization continues and, where they support our accounting and tax records, for six years after the end of the tax year they relate to, which is the period the Income Tax Act requires;

- Platform account information: for the life of the client's subscription, then deleted within ninety (90) days of termination unless the law requires longer;
- Platform activity and audit logs: twelve (12) months; infrastructure request logs used for security and troubleshooting: no longer than twelve (12) months;
- website analytics: in aggregated reports only.

Client Data is returned or deleted in accordance with the client's agreement, which also sets out what happens when a client cancels: the client may export its data, and we then delete it.

10. How we protect information

We implement administrative, technical, and physical safeguards appropriate to the sensitivity of the information. On the Platform these include encryption in transit (TLS 1.2 or higher), encryption at rest, application-layer encryption of designated personal-information fields such as donor email addresses, phone numbers, and postal addresses, database-level isolation of each client's data from every other client's, individual user accounts with hashed passwords, and least-privilege access to production systems for the people who need it. No system is perfectly secure, and we cannot guarantee the security of information transmitted to or from the Sites or the Platform.

11. If something goes wrong

If we become aware of a breach of security safeguards involving personal information, we will contain and investigate it, notify the affected client organizations without undue delay with the information they need to meet their own obligations, notify the Office of the Privacy Commissioner of Canada, any applicable provincial commissioner, and affected individuals where the law requires it, and take reasonable steps to prevent a recurrence. We keep a record of every breach of security safeguards, whether or not it meets the reporting threshold, for at least twenty-four (24) months, as the Breach of Security Safeguards Regulations require.

12. Your rights in Canada

If you are in Canada, you have the right, under the Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial legislation (including Quebec's private-sector privacy act as amended by Law 25, the BC Personal Information Protection Act, and the Alberta Personal Information Protection Act), to:

- access the personal information we hold about you;
- ask us to correct inaccurate or incomplete information;
- withdraw your consent to our use of your information, subject to legal and contractual limits, and to have it deleted where we have no legal reason to keep it;
- in Quebec, receive your information in a structured, commonly used format, and be informed of any decision based exclusively on automated processing (we make none); and

- file a complaint with the Office of the Privacy Commissioner of Canada or your provincial commissioner (in Quebec, the Commission d'accès à l'information).

If your personal information is in a client's records on the Platform, direct your request to that organization; it is the accountable organization, and we will help it respond.

To exercise any of these rights, email our Privacy Officer at the address in Section 17. We will verify your identity and respond within thirty (30) days, or tell you if we need longer and why.

13. Your rights in the United States

If you are a resident of California, Virginia, Colorado, Connecticut, Utah, Texas, or another United States state with a consumer privacy law, you have the following rights, subject to limits in the applicable law: to know what personal information we have about you and how we use it; to access a copy of it; to correct it; to delete it; to opt out of sale or sharing (we do neither); to limit the use of sensitive personal information (we do not use it for purposes that would trigger this right); to data portability in certain circumstances; and to non-discrimination for exercising your rights.

To exercise these rights, email us at the address in Section 17. We will verify your identity and respond within the time the applicable law requires, generally forty-five (45) days for California with a possible forty-five (45) day extension. You may designate an authorized agent to make a request on your behalf; we will require proof of the agent's authorization and may verify your identity directly. If we deny a request, you can appeal by replying to our response with the word "Appeal" and your reasoning. California residents may also contact the California Attorney General's office.

14. Marketing communications

You can unsubscribe from marketing emails at any time using the link in any email or by emailing us. We will continue to send service communications necessary to administer your account. Our marketing emails comply with Canada's Anti-Spam Legislation (CASL) and the United States CAN-SPAM Act.

15. Children's privacy

The Sites and the Platform are directed at organizations and their authorized representatives, not at children. We do not knowingly collect personal information from children under 13 in the United States or under the age of majority in a Canadian province. If you believe we have inadvertently collected information from a child, contact us and we will delete it.

16. The Standard and Sovereign Data Configurations

Every client receives the Standard Data Configuration described in this Policy: data stored and processed at rest in Canada, encryption and client isolation, no sale of data, no AI training on data, AI processing in the United States under no-training terms, and the rights set out above. These are our commitments to every client and they meet Canadian privacy law.

The Sovereign Data Configuration adds commitments that go beyond what the law requires and that change how we run the service: a dedicated, single-tenant deployment with its own encryption key, used for no other client, on AWS in Canada or on Goodfinity's own hardware in Kelowna, British Columbia; AI processing on open-source models hosted on Goodfinity's own hardware in Kelowna, British Columbia, with any cloud provider used only on the client's recorded consent and no AI request at all until a consent policy covers it; no secondary use or cross-client aggregation of any kind; a governance layer in which the client's designated authority approves data flows before they happen; access to an immutable audit log; and defined export and verified-deletion commitments. It is designed around the First Nations principles of OCAP® (Ownership, Control, Access, Possession) and is offered to First Nations, tribal councils, Indigenous organizations, and any other client that contracts for it.

The Sovereign Data Configuration applies only where a client's Order Form or Statement of Work designates it. It is priced to reflect the dedicated infrastructure and governance work it involves, and it cannot be elected after the fact or by request. The Sovereign Data Privacy Policy, published at goodfinity.ca/sovereign-data-privacy, describes it in full.

17. Contact us

Goodfinity's Privacy Officer is the person in charge of the protection of personal information for the purposes of PIPEDA and Quebec's privacy act. The Privacy Officer is Brandon Farr, founder of Goodfinity.

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

18. Changes to this policy

We may update this Policy from time to time. When we do, we will change the "Last modified" date at the top and, where the law requires it, give additional notice, for example by email or a prominent notice on the Sites or in the Platform. We review this Policy at least once a year.