Goodfinity Data Processing Agreement

Last modified:October 29, 2026

This Data Processing Agreement ("DPA") is the "Cloud Data Processing Addendum" referred to in the Goodfinity Terms of Service. It forms part of the Goodfinity Terms of Service (the "Agreement") between Goodfinity, a division of Level Up Strategies Inc. ("Goodfinity", "we"), and the customer organization that has accepted the Agreement ("Customer", "you"). It governs Goodfinity's processing of Customer Data on the Customer's behalf. If there is a conflict between this DPA and the rest of the Agreement on the subject of data processing, this DPA controls.

1. Roles and Scopes

1.1 Accountability. The Customer is the organization accountable for the personal information contained in Customer Data under Canada's *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). Goodfinity processes Customer Data only as a service provider acting on the Customer's behalf and instructions, consistent with PIPEDA Principle 4.1.3 (an organization remains accountable for personal information transferred to a third party for processing).

1.2 What this DPA covers. This DPA covers Customer Data: the data a Customer or its authorized users submit to, store in, or generate through the Platform, including uploaded documents and the normalized donor, donation, contact, program, and financial records derived from them, some of which is personal information about the Customer's own donors, staff, and constituents ("Customer Personal Data").

1.3 What this DPA does not cover. Personal information for which Goodfinity is the accountable organization, chiefly the account and usage information of the Customer's users, is governed by the Goodfinity Privacy Policy, not this DPA.

1.4 Data configurations. This DPA describes the Standard Data Configuration. The Sovereign Data Configuration, with the additional commitments in the Sovereign Data Privacy Policy, applies only to a deployment that an Order Form, Statement of Work or Sovereign Data Rider designates, and cannot be elected by request.

2. Processing Instructions

2.1 Goodfinity will process Customer Personal Data only: - to provide, secure, and support the Services as described in the Agreement; - in accordance with the Customer's documented instructions (the Customer's configuration and use of the Platform constitutes such instructions); and - as required by applicable law, in which case Goodfinity will inform the Customer of the requirement before processing, unless the law prohibits it.

2.2 Goodfinity will not use Customer Personal Data for its own purposes, will not sell it, and will not use it for advertising. Goodfinity will not use Customer Personal Data to train or fine-tune general-purpose AI models. Goodfinity has requested a Zero Data Retention addendum with its AI sub-processor (Anthropic, Annex B); until it takes effect, query text and document context sent to the AI service are handled under Anthropic's standard commercial API terms, which do not use them to train Anthropic's models and provide for deletion after a limited retention period.

2.3 If Goodfinity believes an instruction violates PIPEDA or other applicable law, it will notify the Customer.

3. Confidentiality

Goodfinity will ensure that personnel authorized to process Customer Personal Data are bound by confidentiality obligations and access it only on a need-to-know basis.

4. Security Measures

Goodfinity will maintain the technical and organizational safeguards described in **Annex C**, appropriate to the sensitivity of the data. These include application-layer encryption of designated personal-information fields, database-level access isolation, encryption in transit, and authentication controls. Goodfinity may update specific measures over time provided the overall level of protection is not reduced.

5. Sub-Processors

5.1 Authorization. The Customer authorizes Goodfinity to engage the sub-processors listed in **Annex B** to process Customer Personal Data in connection with the Services.

5.2 Flow-down. Goodfinity will impose data-protection and security obligations on each sub-processor that are substantially consistent with those in this DPA, and remains responsible for each sub-processor's performance.

5.3 Changes. Goodfinity will give the Customer notice before adding or replacing a sub-processor that processes Customer Personal Data. If the Customer reasonably objects on data-protection grounds, the parties will work in good faith to resolve the concern; if they cannot, the Customer may terminate the affected Services.

5.4 Optional integrations. Where the Customer connects an external data source (QuickBooks Online, Google Drive, Microsoft OneDrive/SharePoint, or a supported CRM), that third party is not a Goodfinity sub-processor; the Customer's use of it is governed by the Customer's own agreement with that provider. These integrations are off by default and activate only on the Customer's authorization.

6. Cross-Border Processing

6.1 The platform, including its database, its application and background services, and its uploaded-document storage, is hosted with Amazon Web Services in Canada (ca-central-1), so Customer Personal Data is stored and processed at rest in Canada. Some processing occurs outside Canada: AI processing uses Anthropic Claude (a United States company) and transactional email is sent via Google Workspace, which offers no Canadian data region, so mail is held in Google's data centres and may be outside Canada. Network traffic to and from the platform passes through Cloudflare's edge network in transit. See Annex B. The Customer acknowledges and instructs this processing.

6.2 While Customer Personal Data is in another jurisdiction, it may be subject to lawful access by that jurisdiction's courts, law enforcement, and government authorities. Goodfinity applies the safeguards in Annex C and the flow-down obligations in Section 5 to protect it, consistent with PIPEDA's requirement that transferred data receive a comparable level of protection.

7. Assistance to the Customer

7.1 Access and correction requests. If an individual contacts Goodfinity to access or correct personal information that is Customer Personal Data, Goodfinity will refer the individual to the Customer and will, taking into account the nature of the processing, provide reasonable assistance to help the Customer respond.

7.2 Regulatory and legal requests. Unless legally prohibited, Goodfinity will inform the Customer of any legally binding request for disclosure of Customer Personal Data and will not respond except on the Customer's instruction or as legally required.

8. Breach Notification

Goodfinity will notify the Customer without undue delay after becoming aware of a breach of security safeguards affecting Customer Personal Data, and will provide the information the Customer reasonably needs to meet its own obligations under PIPEDA (including the real-risk-of-significant-harm assessment and any reporting to the Office of the Privacy Commissioner of Canada and affected individuals). Goodfinity will take reasonable steps to contain and remediate the breach.

9. Audit and Compliance
Goodfinity will make available to the Customer information reasonably necessary to demonstrate compliance with this DPA.

10. Return and Deletion
10.1 On termination or expiry of the Agreement, and on the Customer's request, Goodfinity will delete or return Customer Personal Data in accordance with the Agreement, subject to any retention required by law.

10.2 Goodfinity will delete residual copies within 90 days of termination unless legally required to retain them, in which case it will continue to protect the data and limit processing to the purpose of that legal requirement.

11. Liability
The liability provisions of the Agreement (including the limitation-of-liability section) apply to this DPA.

Annex A: Details of Processing

- **Subject matter:** Provision of the Insights Engine document-processing, analysis, and reporting Platform.
- **Duration:** For the term of the Agreement plus the deletion period in Section 10.
- **Nature and purpose:** Ingestion, parsing, normalization, entity resolution, embedding, AI-assisted search/chat, and report generation.
- **Categories of data subjects:** The Customer's donors, contacts, staff, volunteers, board members, and other individuals appearing in Customer Data.
- **Categories of personal data:** Names, contact details (email, phone, address), donation and giving history, and other fields present in uploaded documents; designated fields are encrypted at rest.
- **Special note:** The Platform is not authorized for health information subject to PIPEDA/PIPA or HIPAA except under a separate executed addendum (consistent with ToS §3.3).

AI data handling: Goodfinity has requested a Zero Data Retention addendum with Anthropic; until it takes effect, inputs and outputs are handled under Anthropic's standard commercial API terms, which do not use them for model training and provide for deletion after a limited retention period.

Not sub-processors: Statistics Canada and the Bank of Canada (public, non-personal economic data only); optional Customer-connected integrations (Section 5.4).

Annex C: Security Measures

- **Encryption at rest:** Designated personal-information fields (e.g., donor email, phone, address) are encrypted at the application layer using AES-256-GCM (authenticated encryption) before storage; searchable fields use a keyed HMAC-SHA256 blind index rather than plaintext.
- **Access isolation:** PostgreSQL Row-Level Security enforces per-Customer data isolation on every request; RLS context is bound to a request-scoped database connection.
- **Authentication:** Passwords hashed with bcrypt; individual accounts with role-based access.
- **Encryption in transit:** TLS (minimum TLS 1.2, enforced at the edge) for all client and service connections.
- **Least privilege:** Production access limited to personnel who require it.
- **Logging:** Application logs retained for security and troubleshooting; secrets and credentials are redacted from logs.
- **AI processing controls:** System prompts are constrained to prevent cross-Customer data access and are instructed not to emit raw PII except on explicit lookup; AI output is sanitized before rendering. Goodfinity has requested a Zero Data Retention addendum with its AI sub-processor (Anthropic); until it takes effect, inputs and outputs are handled under Anthropic's standard commercial API terms, which do not use them to train Anthropic's models and provide for deletion after a limited retention period.

Annex B: Authorized Sub-Processors

Sub-Processor	Purpose	Data involved	Location
Anthropic, PBC (Claude API)	AI search, chat, report generation, analysis	Query text and document context, which may contain personal	**United States**
Amazon Web Services (ca-central-1)	Database hosting, encryption key management, uploaded-	All Customer Data, with designated fields encrypted; uploaded	**Canada (ca-central-1)**
Cloudflare	Secure network tunnel and DNS in front of the platform	Network traffic in transit only; no Customer Data stored	**Global edge network**
Google (Gmail SMTP)	Transactional email	Recipient addresses and message contents	**United States**