Data Processing Agreement

Incorporated into the Master Services Agreement

Effective July 31, 2026

This Data Processing Agreement ("DPA") is incorporated into the Master Services Agreement between Legacy X LLC, a Pennsylvania limited liability company, d/b/a Luminary Impact ("Provider") and Client, and governs Provider's processing of Client Data. If this DPA conflicts with the Agreement on data protection, this DPA controls.

1. Definitions and Data Classes

"Client Data" means all data Client or its users submit to the platform or that Provider processes on Client's behalf. Client Data falls into four classes, and Provider's platform is architected around the distinction:

Class	Definition and handling
Participant Identity Data	Information identifying an individual served by Client, collected through the platform's coded forms. Stored exclusively in the participant identity vault, readable only by Client's own authenticated users, and not readable by Provider's operators, AI systems, or support roles, by database level access control.
Coded Working Data	Program, outcome, and survey data keyed to participant codes, containing no direct identifiers. Used to produce deliverables.
Organizational Data	Client's organizational information: strategy, grant pipeline, financials, brand assets, briefs, documents, and deliverables.
Account and Usage Data	User accounts, activity records, read event records, and billing records needed to operate the service.

2. Roles, Instructions, and Permitted Use

2.1 Client controls its data. Provider processes it only (a) to provide the services described in the Agreement, (b) as documented in Client's requests and platform configuration, and (c) as required by law, with notice to Client where legally permitted.

2.2 Prohibited uses. Provider will not sell Client Data; use it for advertising; use it to train or fine tune any artificial intelligence model, whether Provider's or a third party's; use one client's data in another client's work product; or use Client Data for any purpose other than providing and securing the services. Aggregated, de identified platform statistics that cannot be traced to Client or to any individual may be used to improve the service.

3. Security Measures

Provider maintains the technical and organizational measures described in its Trust and Data Architecture, the current version of which is provided on request and referred to here as the Security Annex. Those measures include:

- Participant identity vault. Identifying information collected through the platform's coded forms is stored in a vault readable only by Client's own authenticated users, enforced by database row level security. Provider's staff, Provider's AI systems, and support roles have no read path. Provider verifies this by direct query under every internal role.
- Intake screening. Submissions and uploads are screened server side for participant identifying information and rejected before storage, so flagged content is not retained even briefly. File types that cannot be content screened require Client's explicit confirmation that they contain no participant identifying information.
- Least privilege access. Operator access to Client's briefs and strategy is limited to assigned operators, enforced at a single application choke point before any organization data loads, with a database backstop. Administrative overrides are permitted but are flagged in session and written to an audit record. They are never silent.
- Access recording. Reads of Client briefs and strategy surfaces by operators, by administrators acting under override, and by Provider's AI production system are recorded as metadata events consisting of actor class, data class, and timestamp. There is no content field by design. The client facing view of these records is in development; until it ships, Client's portal shows the actions taken on Client's requests and states plainly that it does not show reads.
- Delivery gate. No work produced with AI assistance reaches Client without human review and approval. Provider's AI systems have no technical capability to deliver work product to Client or to any third party.
- Cross client isolation. The drafting context assembled for Client's work is drawn from Client's own brief and brand profile only, with no access to any other client's data.
- Encryption in transit and at rest through Provider's infrastructure providers, role based application access, and audit logging of sensitive actions.

Honest scope. The vault and the access controls described above are enforced by database and application access control, including a server side service role restricted to Provider's own server code that database rules do not bind. They are not enforced by client held encryption keys. Provider's claim is that its people and its systems cannot read Client's participant identities, and Provider verifies that claim by query. Provider does not claim that no party could technically do so.

4. Subprocessors

4.1 Client authorizes the subprocessors listed in Provider's Subprocessor Disclosure, which as of the date of this DPA comprises: Anthropic (AI drafting via API), Supabase (database, authentication, and file storage), Vercel (application hosting), Netlify (marketing website hosting), Stripe (payments), Resend (transactional email delivery), and Twilio (SMS messaging, including one time passcodes for account verification). Electronic signature is performed by Provider's own platform and is not a subprocessor.

4.2 Provider will give Client at least thirty (30) days' written notice before adding a subprocessor that will process Client Data. If Client reasonably objects on data protection grounds and the Parties cannot resolve the objection, Client may terminate the affected services without penalty and receive a pro rata refund of prepaid, unused fees.

4.3 Provider remains responsible for its subprocessors' performance and binds them to obligations no less protective than this DPA.

5. Personnel and Confidentiality

Provider limits access to Client Data to personnel who need it to perform, binds all personnel and contractors to written confidentiality obligations before any access is granted, and maintains the assignment scoping controls described in Section 3.

6. Security Incidents and Breach Notification

6.1 "Security Incident" means a confirmed unauthorized access to, or acquisition, disclosure, alteration, or destruction of, Client Data.

6.2 Provider will notify Client of a Security Incident without undue delay and in no event later than seventy two (72) hours after Provider confirms the incident, by email to Client's designated contact, describing to the extent then known the nature and scope of the incident, the data classes affected, the measures taken or planned, and a Provider contact.

6.3 Provider will cooperate reasonably with Client's own notification obligations, including obligations under Pennsylvania's Breach of Personal Information Notification Act and any funder requirements, provide updates as material facts develop, and will not publicly characterize the incident in a way that names Client without Client's consent, except as required by law.

6.4 Notification is not an admission of fault or liability.

7. Retention, Return, and Deletion

7.1 During the term, Provider retains Client Data as needed to provide the services.

7.2 Export. At any time during the term and for thirty (30) days after termination, Client may export its deliverables and data in commonly usable formats, self serve or on request, at no charge.

7.3 Deletion. Provider will delete Client Data from active systems within sixty (60) days after termination, or earlier on Client's written request after export, and from backup rotations within ninety (90) days of that deletion, and will confirm completion in writing. Provider may retain records it is legally required to keep, for example billing records, which remain protected under this DPA.

8. Audit Support

Not more than once per twelve (12) months, and additionally following a Security Incident affecting Client, Provider will (a) complete Client's or Client's funder's reasonable security questionnaire, and (b) provide the Security Annex and summaries of relevant controls and access records for Client's data. On site or system level audits are not offered at Provider's current scale. Provider will not unreasonably withhold cooperation with a regulator having jurisdiction.

9. Regulated Program Data

9.1 The platform is designed so that Provider does not receive identifying participant information. Client agrees not to submit data subject to heightened federal confidentiality regimes, including identifying information about victims of domestic violence, dating violence, sexual assault, or stalking under VAWA, 34 U.S.C. section 12291(b)(2); patient records subject to 42 C.F.R. Part 2; or protected health information absent an executed Business Associate Agreement, except in coded, de identified form through the platform's designed paths.

9.2 If Client's funding imposes data location or data handling requirements the platform cannot meet, Client will inform Provider and the Parties will structure the engagement so the affected data remains in Client's systems, with Provider working only from coded or aggregate exports. Provider would rather narrow scope than put Client's funding at risk.

10. Liability and Order of Precedence

Liability under this DPA is subject to the Agreement's limitation of liability, including its data protection super cap. This DPA controls over the Agreement on data protection matters. An executed Business Associate Agreement controls over this DPA with respect to protected health information.