Strong Family Program Data Processing Agreement

Version 6 · Last Updated: October 20, 2026

This Strong Family Program Data Processing Agreement (this "**DPA**") is an addendum to the Strong Family Program General Terms (the "**General Terms**") entered into between GO Project and Partner and is hereby incorporated into and made part of the General Terms and the Agreement (as defined therein). Any capitalized terms used but not defined in this DPA shall have the meanings set forth in the General Terms or the Agreement, as applicable in context.

WHEREAS, the Agreement and General Terms may require GO Project to process certain Personal Information provided by or collected for Partner; and

WHEREAS, this DPA sets out the additional terms, requirements, and conditions on which GO Project will obtain, handle, process, disclose, transfer, or store Personal Information when providing the Application, Strong Family Materials, Strong Family Platform, and related services under the Agreement and General Terms;

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree as follows:

1. Definitions and Interpretation

1.1 The following definitions and rules of interpretation apply in this DPA.

"**Authorized Persons**" means the persons or categories of persons that Partner authorizes to give GO Project Personal Information processing instructions, including Partner's Authorized Users (as defined in the General Terms).

"**Business Purpose**" means provision of the Strong Family Program, the Application, the Strong Family Platform, and Strong Family Materials to Partner and related services described in the Agreement and General Terms, or any other purpose specifically identified in Appendix A.

"**Data Subject**" means an individual who is the subject of the Personal Information and to whom or about whom the Personal Information relates or identifies, directly or indirectly.

"**Personal Information**" means any individually identifiable information GO Project Processes on behalf of Partner in connection with the Business Purpose that (a) identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in GO Project's possession or control or that GO Project is likely to have access to, or (b) the relevant Privacy and Data Protection Requirements otherwise define as protected personal information. Personal Information may include, but is not limited to: (i) identifying information (e.g., name, date of birth, gender, and family relationships); (ii) contact information (e.g., address, telephone number, and email address); (iii) individual and family wellness data (including health, nutrition, education, economic, psychological, social, and spiritual well-being information); (iv) assessment results, case notes, and progress reports; (v) photographs or images; (vi) sensitive personal data, which may include information relating to health, religion, ethnicity, or other categories of data considered sensitive under the laws of the applicable jurisdiction; and (vii) other information provided by or about Participants through the Application or Strong Family Platform in connection with program participation. For clarity, Personal Information does not include (x) De-Identified Data, (y) Aggregated Statistics, or (z) any information Processed in connection with GO Project Independent Processing (as defined below), regardless of whether such information would otherwise satisfy the definition of "Personal Information" in the absence of this subsection (z).

"**De-Identified Data**" means information derived from Personal Information that does not identify a Data Subject and cannot reasonably be used, alone or in combination with other information, to identify a Data Subject.

"**Aggregated Statistics**" has the meaning given in the General Terms and includes aggregated and anonymized statistical and performance information relating to the provision and operation of the Application.

"**GO Project Independent Processing**" means Processing by GO Project for GO Project's own independent purposes (and not on behalf of Partner) where and to the extent such Processing is permitted under the Agreement and General Terms and is supported by a lawful basis under applicable Privacy and Data Protection Requirements (including, where applicable, a valid consent by the Participant to GO Project's Processing for such purposes).

"**Participant Consent Form**" means the Strong Family Program participant consent provided by GO Project for use by Partner, including the consent presented in the Application during each annual data collection window (as may be updated by GO Project

from time to time consistent with applicable law), to obtain Participant consent for collection, use, transfer, and other Processing of Participant personal data.

"**Processing, processes, or process**" means any activity that involves the use of Personal Information or that the relevant Privacy and Data Protection Requirements may otherwise include in the definition of processing, processes, or process. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including, but not limited to, organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Information to third parties.

"**Privacy and Data Protection Requirements**" means all applicable federal, state, and foreign laws and regulations relating to the processing, protection, or privacy of the Personal Information, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction.

"**Security Breach**" means any act or omission that compromises the security, confidentiality, or integrity of Personal Information or the physical, technical, administrative, or organizational safeguards put in place to protect it. The loss of or unauthorized access, disclosure, or acquisition of Personal Information is a Security Breach whether or not the incident rises to the level of a security breach under the Privacy and Data Protection Requirements.

1.2 This DPA is subject to the terms of the General Terms and the Agreement and is incorporated into the Agreement. Interpretations and defined terms set forth in the General Terms and the Agreement apply to the interpretation of this DPA.

1.3 The Appendices form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Appendices.

1.4 A reference to writing or written includes email.

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this DPA and any provision contained in the Appendices, the provision in the body of this DPA will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this DPA and any provision contained in the Appendices, the provision contained in the Appendices will prevail;

(c) any of the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA will prevail; and

(d) any of the provisions of this DPA and any applicable cross-border data transfer agreement executed by the parties, the provisions of such cross-border data transfer agreement will prevail.

2. Personal Information Types and Processing Purposes

2.1 Partner retains control of the Personal Information and remains responsible for its compliance obligations under the applicable Privacy and Data Protection Requirements, including providing any required notices and obtaining and maintaining any required consents (including using the Participant Consent Form where required under the Agreement or applicable law), and for the processing instructions it gives to GO Project. For the Business Purpose, Partner acts as the data controller and GO Project acts as the data processor. For GO Project Independent Processing, GO Project acts as an independent data controller. Nothing in the General Terms regarding ownership of Application Data changes these roles or the rights of Data Subjects.

2.2 Appendix A describes the general Personal Information categories and related types of Data Subjects GO Project may Process on behalf of Partner to fulfill the Business Purposes of the Agreement. Partner discloses Personal Information to GO Project only for the limited and specified Business Purposes.

2.3 Nothing in this DPA restricts GO Project from creating, collecting, compiling, or using Aggregated Statistics and/or De-Identified Data, including to improve the Application, Strong Family Materials, Strong Family Platform, and GO Project's products and services, to conduct analytics, and for other lawful purposes, in each case in compliance with the Privacy and Data Protection Requirements.

2.4 To the extent the Agreement and General Terms permit GO Project to use identifiable Application Data for GO Project's own independent purposes (e.g., program evaluation, research, reporting, fundraising, and improvement of GO Project's products and services), such Processing is GO Project Independent Processing and is outside the scope of this DPA unless and to the extent the parties expressly identify it as a Business Purpose in Appendix A. Partner is responsible for providing any required notices and obtaining and maintaining any required consents, authorizations, or other permissions (including, where applicable, execution of the Participant Consent Form) for such GO Project Independent Processing under the Privacy and Data Protection Requirements.

3. GO Project's Obligations

3.1 Subject to Sections 2.3 and 2.4, GO Project will only process, retain, use, or disclose the Personal Information to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with Partner's written instructions from Authorized Persons. GO Project will not process, retain, use, or disclose the Personal Information for any other purpose, outside of the parties' business relationship, or in a way that does not comply with this DPA or the Privacy and Data Protection Requirements. This includes not combining or updating the Personal Information with personal information obtained outside of this contract unless the Privacy and Data Protection Requirements permit the action. GO Project must promptly notify Partner if, in its opinion, Partner's instruction would not comply with the Privacy and Data Protection Requirements.

3.2 GO Project will use commercially reasonable efforts to promptly comply with any Partner request or instruction from Authorized Persons requiring GO Project to amend, transfer, or delete the Personal Information, or to stop, mitigate, or remedy any unauthorized processing, in each case to the extent reasonably feasible.

3.3 GO Project will maintain the confidentiality of all Personal Information and will not sell it to anyone, share it for cross-context behavioral advertising (targeted advertising) with anyone, or disclose it to third parties without specific authorization from Partner or this DPA, unless required by law. If a law requires GO Project to process or disclose Personal Information, GO Project must first inform Partner of the legal requirement and give Partner an opportunity to object or challenge the requirement, unless the law prohibits such notice.

3.4 GO Project will reasonably assist Partner with meeting Partner's compliance obligations under the Privacy and Data Protection Requirements, taking into account the nature of GO Project's processing and the information available to GO Project.

3.5 GO Project must promptly notify Partner of any changes to Privacy and Data Protection Requirements, or its ability to meet those obligations, that may adversely affect GO Project's performance of the Agreement or this DPA.

3.6 Partner acknowledges that GO Project is under no duty to investigate the completeness, accuracy, or sufficiency of any specific Partner instructions from Authorized Persons or the Personal Information other than as required under the Privacy and Data Protection Requirements.

3.7 Personal Information of Data Subjects will be collected through the Application using the Participant Consent Form and the Strong Family Application Privacy Notice available at strongfamily.org/compliance, each as updated by GO Project from time to time, or using another notice or method that Partner specifically pre-approves in writing. Partner acknowledges that these documents identify Partner generically as the local implementing partner, and Partner shall ensure that its Authorized Users tell each Data Subject Partner's name when presenting them.

3.8 GO Project will notify Partner promptly if it receives a legally binding request from a governmental authority (including judicial authorities) to disclose Personal Information Processed on behalf of Partner, or if it becomes aware of any direct access by a governmental authority to such Personal Information, in each case to the extent permitted by law. Such notice will include, to the extent available and legally permissible, the Personal Information requested or accessed, the requesting authority, the asserted legal basis, and GO Project's response.

3.9 When responding to any governmental authority request described in Section 3.8, GO Project will (a) review the request for legality; (b) where GO Project determines there are reasonable grounds to do so, use commercially reasonable efforts to challenge or seek appropriate limitation of the request (including pursuing appeal options as reasonable under the circumstances); and (c) disclose only the minimum amount of Personal Information GO Project is legally required to disclose, based on a reasonable interpretation of the request. GO Project will document its assessment and any challenge or limitation efforts and, to the extent legally permissible, make such documentation available to Partner upon request.

3.10 GO Project will notify Partner promptly if, for the duration of the Term, it has reason to believe that applicable laws or practices (including as evidenced by a governmental authority request) prevent GO Project from complying with this DPA in any material respect. Following such notice, the parties will cooperate in good faith to identify and implement commercially reasonable measures to address the situation (including additional technical or organizational safeguards). If the parties cannot agree on measures that address the issue within a reasonable time, Partner may suspend the relevant Processing and/or terminate the applicable services under the Agreement to the extent necessary to comply with the Privacy and Data Protection Requirements.

4. GO Project's Employees

4.1 GO Project will limit Personal Information access to:

(a) those employees who require Personal Information access to meet GO Project's obligations under this DPA and the Agreement; and

(b) the part or parts of the Personal Information that those employees strictly require for the performance of their duties.

4.2 GO Project will ensure that all employees:

(a) are informed of the Personal Information's confidential nature and use restrictions and are obliged to keep the Personal Information confidential;

(b) have undertaken training on the Privacy and Data Protection Requirements relating to handling Personal Information and how it applies to their particular duties; and

(c) are aware both of GO Project's duties and their personal duties and obligations under the Privacy and Data Protection Requirements and this DPA.

4.3 GO Project will take reasonable steps to ensure the reliability, integrity, and trustworthiness of all of GO Project's employees with access to the Personal Information.

5. Security

5.1 GO Project must at all times implement appropriate technical and organizational measures designed to safeguard Personal Information against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, destruction, unavailability, or damage, including, but not limited to, the security measures set out in Appendix B. In assessing and implementing such measures, GO Project will take due account of the state of the art, the costs of implementation, the nature, scope, context, and purposes of Processing, and the risks to Data Subjects, and will consider the use of encryption and/or pseudonymization where appropriate. GO Project must document those measures in writing and periodically review them, at least annually, to ensure they remain current and complete.

5.2 GO Project will promptly notify Partner if it becomes aware of any material advance in technology and methods of working that is reasonably likely to indicate that the parties should adjust their security measures.

5.3 GO Project must take reasonable precautions to preserve the integrity of any Personal Information it processes and to prevent any corruption or loss of the Personal Information, including but not limited to establishing effective back-up and data restoration procedures.

6. Security Breaches and Personal Information Loss

6.1 GO Project will promptly notify Partner if any Personal Information is lost or destroyed or becomes damaged, corrupted, or unusable. GO Project will use commercially reasonable efforts to restore such Personal Information at its own expense.

6.2 GO Project will within seventy-two (72) hours notify Partner if it becomes aware of any of the occurrences described in Sections 6.2(a) or 6.2(b). Such notification will include, to the extent information is available to GO Project at the time, (i) a contact point for follow-up, (ii) a description of the nature of the incident (including, where possible, categories and approximate number of impacted Data Subjects and Personal Information records), (iii) likely consequences, and (iv) measures taken or proposed to address and mitigate the incident. If all such information cannot be provided at once, GO Project will provide the information then available and provide further information as it becomes available, without undue delay.

(a) any unauthorized or unlawful processing of the Personal Information; or

(b) any Security Breach.

6.3 Immediately following any unauthorized or unlawful Personal Information processing or Security Breach, the parties will coordinate with each other to investigate the matter. GO Project will reasonably cooperate with Partner in Partner's handling of the matter, including:

(a) assisting with any investigation;

(b) providing Partner with reasonable physical and/or remote access (as appropriate under the circumstances) to any facilities and operations affected, subject to GO Project's reasonable safety, security, and confidentiality requirements;

(c) facilitating interviews with GO Project's employees, former employees, and others involved in the matter; and

(d) making available all relevant records, logs, files, data reporting, and other materials reasonably necessary and proportionate to comply with all Privacy and Data Protection Requirements or to support Partner's reasonable response, in each case subject to GO Project's confidentiality and security obligations.

6.4 GO Project will not inform any third party of a Security Breach without first obtaining Partner's prior written consent, except (a) when law or regulation requires it; (b) to the extent necessary to engage GO Project's and its subcontractors', professional advisors',

or insurers' services in connection with the Security Breach; or (c) where disclosure is otherwise necessary to address or mitigate the Security Breach, in each case to the extent permitted by law and subject to reasonable confidentiality protections.

6.5 GO Project agrees that Partner has the sole right to determine:

(a) whether to provide notice of the Security Breach to any Data Subjects, regulators, law enforcement agencies, or others, as required by law or regulation or in Partner's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

7. Cross-Border Transfers of Personal Information

7.1 GO Project acknowledges that Personal Information may originate from countries outside the United States that impose restrictions on cross-border data transfers. If the Privacy and Data Protection Requirements restrict cross-border Personal Information transfers, Partner will only transfer that Personal Information to GO Project under the following conditions:

(a) GO Project, either through its location or participation in a valid cross-border transfer mechanism under the Privacy and Data Protection Requirements, as identified in Appendix A, may legally receive that Personal Information, and GO Project must promptly inform Partner of any change to that status;

(b) Partner obtained valid Data Subject consent to the transfer under the Privacy and Data Protection Requirements; or

(c) the transfer otherwise complies with the Privacy and Data Protection Requirements for the reasons set forth in Appendix A.

7.2 If any Personal Information transfer between GO Project and Partner requires execution of additional data transfer agreements or mechanisms in order to comply with the Privacy and Data Protection Requirements, the parties will negotiate in good faith and execute such agreements or mechanisms, and take all other actions reasonably required to legitimize the transfer.

7.3 GO Project will not transfer any Personal Information to another country unless the transfer complies with the Privacy and Data Protection Requirements.

8. Subcontractors

8.1 GO Project may only authorize a third party (subcontractor) to process the Personal Information if:

(a) Partner is given an opportunity to object within thirty (30) days after GO Project supplies Partner with full details regarding such subcontractor;

(b) GO Project enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this DPA with respect to Personal Information, and, upon Partner's written request, provides Partner with a written summary of the relevant data protection terms and, to the extent reasonably necessary and legally permissible, redacted copies of such contracts;

(c) GO Project maintains control over all Personal Information it entrusts to the subcontractor; and

(d) the subcontractor's contract requires the subcontractor, upon termination or expiration of the subcontract, to cease Processing and securely return and/or destroy the Personal Information in accordance with instructions from GO Project consistent with this DPA.

8.2 GO Project must list all approved subcontractors in Appendix A and include each subcontractor's name, service, and location. GO Project will provide contact information for a subcontractor's privacy and data protection function upon Partner's written request.

8.3 Where the subcontractor fails to fulfill its obligations under such written agreement, GO Project remains fully responsible to Partner for the subcontractor's performance of its agreement obligations.

8.4 The parties consider GO Project to control any Personal Information controlled by or in the possession of its subcontractors.

8.5 Upon Partner's written request, if permitted by the applicable subcontractor, GO Project will use commercially reasonable efforts to obtain and provide to Partner available audit reports, certifications, and/or other reasonable assurances regarding the subcontractor's compliance with its obligations regarding Partner's Personal Information, and, where reasonably necessary, may audit such subcontractor's compliance (which audit may be conducted remotely) and provide Partner with the results.

9. Data Subject Requests, Complaints, and Third Party Rights

9.1 GO Project must notify Partner within five (5) working days if it receives a request from a Data Subject to exercise any rights the individual may have regarding their Personal Information, such as access, correction, deletion, or to opt-out of or limit certain activities like sales, disclosures, or other processing actions.

9.2 GO Project must notify Partner promptly, and in any event within five (5) working days, if it receives any other complaint, notice, or communication that directly or indirectly relates to the Personal Information processing or to either party's compliance with the Privacy and Data Protection Requirements.

9.3 GO Project will provide Partner its reasonable cooperation and assistance in responding to any complaint, notice, communication, or Data Subject request.

9.4 GO Project must not disclose the Personal Information to any Data Subject or to a third party unless the disclosure is either at Partner's request or instruction, permitted by this DPA, or is otherwise required by law.

10. Term and Termination

10.1 This DPA will remain in full force and effect so long as:

(a) the Agreement remains in effect; or

(b) GO Project retains any Personal Information related to the Agreement in its possession or control (collectively, the "**Term**").

10.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Agreement in order to protect Personal Information will remain in full force and effect.

10.3 GO Project's failure to comply with the terms of this DPA is a material breach of the Agreement. In such event, Partner may terminate the Agreement upon written notice (not to include email) to GO Project if GO Project fails to cure such material breach within thirty (30) days after receipt of such notice; provided that no cure period will apply where the breach is incapable of cure or relates to a Security Breach or unlawful Processing of Personal Information.

10.4 If a change in any Privacy and Data Protection Requirement or either party's circumstances prevents a party from fulfilling all or part of its Agreement obligations, the parties will suspend the processing of Personal Information until the party's processing complies with the requirements. If the parties are unable to bring the Personal

Information processing into compliance with the Privacy and Data Protection Requirements within ninety (90) days of such change, either party may terminate the Agreement upon written notice to the other party.

11. Data Return and Destruction

11.1 At Partner's request, GO Project will provide Partner a copy of or access to all or part of Partner's Personal Information in its possession or control in a format and on media reasonably specified by Partner, to the extent technically feasible.

11.2 On termination of the Agreement for any reason or expiration of its term, GO Project will securely destroy or, if directed in writing by Partner, return and not retain, all or any Personal Information related to this agreement in its possession or control, except for one copy that it may retain and use for twelve (12) months for audit and compliance purposes only.

11.3 If any law, regulation, or government or regulatory body requires GO Project to retain any documents or materials that GO Project would otherwise be required to return or destroy, it will notify Partner in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends. GO Project may only use this retained Personal Information for the required retention reason or audit purposes.

11.4 GO Project will certify in writing that it has destroyed the Personal Information within thirty (30) days after it completes the destruction.

12. Records

12.1 GO Project will keep reasonably detailed, accurate, and up-to-date records regarding any Processing of Personal Information it carries out for Partner, including the access, control, and security of the Personal Information, approved subcontractors and affiliates, processing purposes, and any other records required by the applicable Privacy and Data Protection Requirements (the "**Records**").

12.2 GO Project will use commercially reasonable efforts to ensure that the Records are sufficient to enable Partner to verify GO Project's compliance with its obligations under this DPA.

12.3 Partner and GO Project must regularly review the information listed in the Appendices to this DPA to confirm its current accuracy and update it when required to reflect current practices.

13. Documentation and Compliance Reviews

13.1 GO Project will make available to Partner, upon written request, information reasonably necessary to demonstrate GO Project's compliance with this DPA, which may include written summaries of relevant policies and procedures, descriptions of technical and organizational measures, and the then-current list of subcontractors authorized to process Personal Information on behalf of GO Project.

11.5 On termination or expiration of the Agreement, and upon Partner's written request within thirty (30) days thereafter, GO Project will provide Partner with one export, in a commonly used electronic format, of the Application Data relating to Participants served by Partner, solely for Partner's continued support of those Participants. Partner shall protect the exported data in accordance with the confidentiality and data protection obligations of the General Terms, this DPA, and the Participant consent, which survive termination for this purpose.

13.2 To the extent available, GO Project may satisfy its obligations under this Section 13 by providing Partner with copies (or summaries, where full copies are not reasonably available due to confidentiality obligations) of third-party certifications, audit reports, or assessments addressing GO Project's information security program, including SOC, ISO/IEC 27001, and/or comparable reports, and by providing an annual written attestation regarding its compliance with this DPA.

13.3 If the information made available under this Section 13 is not reasonably sufficient to address Partner's reasonable compliance concerns, Partner may request an audit of GO Project's processing activities under this DPA at reasonable intervals or where there are indications of non-compliance; provided that (a) the parties will first seek to address the request through remote review of documentation and reasonable Q&A, (b) any on-site inspection will occur only where remote review is not reasonably sufficient, (c) any audit will be subject to reasonable advance notice, scope limitations, and GO Project's confidentiality and security requirements, (d) any audit will be conducted during normal business hours in a manner designed to minimize disruption, and (e) Partner will bear its own audit costs (and, if it engages a third-party auditor, will ensure the auditor is bound

by written confidentiality obligations) unless the audit identifies a material breach of this DPA by GO Project, in which case the parties will discuss in good faith an appropriate allocation of reasonable audit costs.

14. Data Protection Impact Assessments

Considering the nature of the processing under the Agreement, GO Project will provide reasonable assistance to Partner with any data protection impact assessments, and with any prior consultations with regulators or other authorities, that GO Project reasonably considers to be required by applicable Privacy and Data Protection Requirements. Such assistance may include providing information regarding GO Project's processing operations, technical and organizational measures, and the potential risks to the rights of Data Subjects.

15. Warranties

Partner warrants and represents that GO Project's expected use of the Personal Information for the Business Purpose and as specifically instructed by Partner will comply with all Privacy and Data Protection Requirements.

16. Notice

Any notice or other communication given to a party under or in connection with this DPA must be in writing and delivered to the respective parties at the addresses set forth in the Agreement (or to such other address as may be designated by a party from time to time in accordance with the Agreement and/or General Terms, as applicable). This Section 16 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution. A notice given under this DPA by GO Project may be sent to Partner via email to the address specified under the Agreement.

17. Modifications

Partner acknowledges and agrees that GO Project has the right, in GO Project's sole discretion, to modify this DPA from time to time, and that modified terms become effective on posting at strongfamily.org/compliance. Partner is responsible for reviewing and becoming familiar with any such modifications. Partner's continued use of the

Application, Strong Family Platform, or Strong Family Materials or sharing of Personal Information after the effective date of the modifications will be deemed acceptance of the modified terms.

Appendix A – Personal Information Processing Purposes and Details

Business Purposes: Providing the Strong Family Program, including the Strong Family Application, Strong Family Platform, Strong Family Materials, and related services as described in the Agreement and General Terms, including the collection, storage, processing, and analysis of Participant and Authorized User data through the Application and Platform for case management, monitoring, follow-up, and administration, evaluation, and improvement of programs and services.

Excluded Data / Additional GO Project Uses: GO Project may create and use Aggregated Statistics and De-Identified Data from Application Data and/or Personal Information for analytics, improvement, and other lawful purposes. In addition, GO Project may conduct GO Project Independent Processing (including program evaluation, research, reporting, fundraising, and improvement of GO Project's products and services) to the extent permitted by the Agreement and General Terms and supported by a lawful basis under applicable Privacy and Data Protection Requirements (including, where applicable, valid Participant consent obtained using the Participant Consent Form).

Personal Information Categories: Identifying information (e.g., name, date of birth, gender, and family relationships); contact information (e.g., address, telephone number, and email address); individual and family wellness data (including health, nutrition, education, economic, psychological, social, and spiritual well-being information); assessment results, case notes, and progress reports; photographs or images; sensitive personal data (which may include information relating to health, religion, ethnicity, or other categories of data considered sensitive under the laws of the applicable jurisdiction); and other information provided by or about Participants through the Application in connection with program participation.

Data Subject Types: Authorized Users, including employees and volunteers of Partner and of Local Church partners; Participants (as defined in the General Terms), including individuals and family members participating in programs administered or facilitated by Partner using the Application.

Processing Duration: For the duration of the Agreement, plus any retention period specified in Section 11.

Approved Subcontractors: The following subcontractors are approved as of the date of this DPA. Any new subcontractors shall be designated in accordance with Section 8.

Subcontractor	Service	Location
Amazon Web Services, Inc.	Hosting and storage for the Application	United States
Databricks, Inc.	Data platform for reporting, analytics, and research	United States
Google LLC (Firebase Crashlytics)	Application crash and error reporting	United States

Authorized Persons: Partner's Authorized Users as designated pursuant to the Agreement and applicable Enrollment Forms.

Countries where GO Project may receive, access, transfer, or store Personal Information: United States of America.

Appendix B – Security Measures

GO Project will implement and maintain the following categories of technical and organizational security measures, as appropriate to the nature of the Personal Information processed:

- Physical access controls designed to prevent unauthorized persons from gaining access to data processing systems.
- System access controls designed to prevent data processing systems from being used without authorization.
- Data access controls designed to ensure that authorized users can only access the Personal Information to which they are entitled and that Personal Information cannot be read, copied, modified, or removed without authorization.
- Transmission controls, including encryption during transmission where applicable, designed to ensure that Personal Information cannot be read, copied, modified, or removed without authorization during electronic transfer or transport.
- Input controls designed to ensure that it is possible to verify and establish whether and by whom Personal Information has been entered into, modified, or removed from data processing systems.

- Data backup and restoration procedures designed to ensure the availability and resilience of Personal Information and the ability to restore access in a timely manner in the event of a physical or technical incident.
- Data segregation controls designed to ensure that Personal Information collected for different purposes is processed separately.