Data Processing Agreement

This Data Processing Agreement (this "**DPA**") is incorporated into and forms part of the Subscription and Services Agreement, Master Subscription Agreement or similar agreement (including any Order Forms, annexes, addendum or schedules attached thereto or URLs referenced therein) entered into between Bonterra LLC or its corresponding affiliate ("**Bonterra**") and the applicable customer identified therein ("**Customer**") (as applicable, the "**Principal Agreement**"). This DPA is effective as of the effective date of the Principal Agreement (the "**Effective Date**") and details the parties' obligations with respect to the Processing of Covered Data on behalf of Customer or its Authorized Affiliate pursuant to the Principal Agreement.

1. Definitions

1.1 "**Affiliate**" means affiliates, subsidiaries, sister companies or entities, related entities, parent entities or a party.

1.2 "**Authorized Affiliate**" means any Affiliate of Customer who (i) is authorized by Customer to use the services supplied by Bonterra in accordance with the Principal Agreement between Customer and Bonterra, and (ii) has not signed its own Order, Statement of Work or other written agreement with Bonterra.

1.3 "**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

1.4 "**Covered Data**" means Personal Data that is provided by or on behalf of Customer to Bonterra in connection with the fulfilment of contractual obligations under the Principal Agreement.

1.5 "**Data Subject**" means the individual to whom Personal Data relates.

1.6 "**Deidentified Data**" means data derived from Personal Data that cannot reasonably be linked to any individual.

1.7 "**Order Form**" means Bonterra's standard order documentation used to purchase Services. An Order may also include a Statement of Work.

1.8 "**Personal Data Breach**" means an actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Covered Data transmitted, stored or otherwise Processed by Bonterra and/or its Subprocessors in connection with the provision of services under the Principal Agreement.

1.9 "**Personal Data**" means any information that identifies or is reasonably linkable to an identified or identifiable natural person.

1.10 "**Process**", "**Processed**", or "**Processing**" means any operation or set of operations which is performed upon Covered Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.11 "**Processor**" means a natural or legal person, public authority, agency or other body that Processes Personal Data on behalf of the Controller.

1.12 "**Statement of Work**" or "**SOW**" means a statement of work or other ordering document between Bonterra and Customer that describes certain type of Services to be furnished by Bonterra.

1.13 "**Subprocessor**" means a natural or legal person, public authority, agency or other body that Processes Personal Data on behalf of the Processor.

2. Relationship of the Parties

2.1 Customer is the Controller of Covered Data. Bonterra processes Covered Data as a Processor acting on Customer's behalf.

2.2 To the extent Bonterra is required by applicable law, regulation, or binding legal process to retain certain Personal Data (*e.g.*, payment records, tax documentation, and transaction records) for its own regulatory or compliance purposes, Bonterra acts as an independent Controller solely for that limited retention. In such capacity, Bonterra will: (a) process the retained Personal Data only for the specific legal purpose requiring its retention; (b) apply technical and organizational safeguards no less protective than those described in Annex II; and (c) retain the Personal Data only for as long as required by the applicable legal obligation.

2.3 Each party shall comply with its applicable obligations under applicable data protection laws. Customer represents that it has all rights and authorizations necessary for Bonterra to process Covered Data.

3. Processing Instructions

3.1 Bonterra will process Covered Data to provide the services described in the Principal Agreement, in accordance with Customer's documented instructions. Customer agrees that applicable provisions of the Principal Agreement and Customer's use and configuration of the features within the licensed Bonterra product constitutes Customer's instructions with respect to Bonterra's Processing of the Covered Data on Customer's behalf. Bonterra shall inform Customer if it believes that any instructions Customer provides infringes applicable data protection laws.

3.2 Customer may issue additional processing instructions by written notice to Bonterra. Bonterra will implement additional instructions that fall within the scope of the Principal Agreement. If an additional instruction requires effort or cost beyond the existing scope, Bonterra may charge a reasonable fee, which the parties will agree to in writing before implementation.

3.3 If Bonterra is required by applicable law to process Covered Data in a manner that conflicts with Customer's instructions, Bonterra will notify Customer before doing so, unless that law prohibits such notice.

3.4 Bonterra will not: (a) retain, use, or disclose Covered Data for any commercial purpose other than providing the services; or (b) combine Covered Data with personal data collected from other sources except as necessary to provide the services.

4. Customer Responsibilities

Customer is responsible for the lawfulness of its processing of Covered Data. Customer will:

(a) provide all required notices and obtain all required consents, permissions, and rights necessary for Bonterra to process Covered Data as described in this DPA and the Principal Agreement;

(b) ensure its instructions to Bonterra comply with applicable law;

(c) take appropriate steps to classify and protect Covered Data before providing it to Bonterra; and

(d) notify Bonterra promptly if Customer becomes aware of any data protection issue arising from its use of licensed Bonterra services.

5. Bonterra's Obligations

5.1 Bonterra will process Covered Data only as necessary to perform its obligations under the Principal Agreement and this DPA, or as required by applicable law.

5.2 Bonterra will keep Covered Data strictly confidential and will ensure that all personnel authorized to process Covered Data are bound by appropriate confidentiality obligations and trained on data protection requirements.

5.3 Unless prohibited by law, Bonterra will notify Customer without undue delay if Bonterra: (a) receives a request, complaint, or inquiry from a Data Subject or supervisory authority regarding Covered Data; (b) receives a request to disclose Covered Data from law enforcement, courts, or any government authority; or (c) determines that it can no longer comply with this DPA.

5.4 Bonterra will inform Customer if, in its opinion, a processing instruction infringes applicable legal requirements.

6. Security and Personal Data Breaches

6.1 Bonterra will implement and maintain appropriate technical and organizational measures to protect Covered Data against Personal Data Breaches. Those measures are described in Annex II. Bonterra may update its security measures from time to time provided that any update does not materially reduce the level of protection in effect at the time Customer signed this DPA.

6.2 Bonterra will notify Customer without undue delay after becoming aware of a Personal Data Breach. That notice will include, to the extent then available: (a) the nature of the breach; (b) the categories and approximate numbers of Data Subjects and records affected; (c) the likely consequences; and (d) the measures taken or proposed to address the breach. Bonterra will provide Customer with updates as additional information becomes available.

6.3 Bonterra's notification of a Personal Data Breach does not constitute an acknowledgment of fault or liability.

7. Data Subject Access Rights Assistance

Bonterra will provide Customer with reasonable assistance in fulfilling Customer's obligations to respond to Data Subject rights requests, including requests to access, correct, delete, restrict, or port Covered Data. If a Data Subject contacts Bonterra directly regarding Covered Data, Bonterra will refer the Data Subject to Customer and will not respond substantively without Customer's instruction.

8. Subprocessors

Customer consents to Bonterra Affiliates being retained as Subprocessors in connection with the provision of services under the Principal Agreement, and to Bonterra's use of third-party Subprocessors. A list of Bonterra's Subprocessors then in effect is available on Bonterra's Trust Center at https://trustcenter.bonterratech.com or other URL as is designated by Bonterra from time to time ("**Trust Center**"). Furthermore, Customer consents to Bonterra engaging additional Subprocessors provided that Bonterra imposes data protection terms on any Subprocessor to the materially equivalent standards provided for by this DPA, and Bonterra remains fully liable for any breach of this DPA that is caused by its Subprocessor.

9. Audits

9.1 Once per calendar year, Customer may audit Bonterra's compliance with this DPA by submitting a written request with at least 30 days' prior notice. Audits must occur during normal business hours, follow an agreed audit plan, and not unreasonably disrupt Bonterra's operations. If Customer uses a third-party auditor, Bonterra may object to the auditor on reasonable grounds, and Customer will appoint an alternate auditor. All audit activities and findings are confidential.

9.2 If Bonterra has an in-scope SOC 2 Type 2, ISO 27001, or equivalent audit report issued within twelve months of Customer's request, and there are no known material changes to the controls audited, Customer agrees to accept that report in lieu of a separate audit.

9.3 Customer bears the cost of any audit it initiates and will reimburse Bonterra for time spent on audit support at Bonterra's then-current professional services rates.

10. Data Return and Deletion

Upon termination or expiration of the Principal Agreement, Bonterra will, at Customer's written request, either return or delete all Covered Data within 90 days of Customer's instruction. Bonterra may retain Covered Data to the extent required by applicable law, and will continue to protect such retained data in accordance with this DPA. This DPA remains in effect until Bonterra completes deletion of all Covered Data.

11. Analytics and Deidentified Data

Bonterra may create Deidentified Data from Covered Data and use it to improve its products, services, and internal research. Bonterra will take reasonable measures to ensure that Deidentified Data cannot be re-identified, and will not attempt to re-identify it.

12. General Provisions

12.1 The liability of either party under this DPA is subject to the limitations and caps set out in the Principal Agreement. The parties' combined liability for all claims arising under this DPA will not exceed the liability cap in the Principal Agreement.

12.2 This DPA may be modified only by a written amendment signed by authorized representatives of both parties.

12.3 If any provision of this DPA is found unenforceable, that provision will be severed, and the remaining provisions will continue in full force.

12.4 In the event of a conflict between this DPA and the Principal Agreement with respect to the processing of Covered Data, this DPA controls.

12.5 This DPA is governed by the law specified in the Principal Agreement, except that Appendix A is governed as specified therein.

12.6 This DPA, together with the Principal Agreement and its exhibits, constitutes the entire agreement of the parties with respect to the processing of Covered Data and supersedes all prior agreements, representations, or understandings on that subject.

Appendix A

Additional Terms: European Economic Area, United Kingdom, and Switzerland

These additional terms apply only where the law of the EEA, the United Kingdom ("**UK**"), or Switzerland governs Customer's transfer of Covered Data to Bonterra. Capitalized terms not defined here have the meanings given in the main DPA.

1. Definitions

"Data Privacy Framework" means the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs (as applicable) operated by the U.S. Department of Commerce, as may be amended, superseded, or replaced.

"EEA" means the European Economic Area.

"EU GDPR" means the EU General Data Protection Regulation (EU) 2016/679.

"**GDPR**" means the EU GDPR and/or UK GDPR, as applicable.

"Restricted Transfer" means: (i) under EU GDPR, a transfer of Covered Data from the EEA to a country without an adequacy decision by the European Commission; and (ii) under UK GDPR, a transfer from the UK to any country without adequacy regulations under the UK Data Protection Act 2018.

"Standard Contractual Clauses" or "SCCs" means the Standard Contractual Clauses annexed to EU Commission Implementing Decision 2021/914 of June 4, 2021, as may be amended or replaced.

"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, version B.1.0.

"**UK GDPR**" means the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018.

2. International Data Transfers

Bonterra may transfer Covered Data outside the EEA or UK when: (a) the recipient is based in a country that the European Commission decided has adequate level of protection for Personal Data, (b) the recipient is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, including the Data Privacy Framework, (c) the recipient obtained binding corporate rules approval according to applicable data protection laws or (d) the SCCs apply.

3. Data Privacy Framework

Customer acknowledges that in connection with the performance of services hired on the Principal Agreement, Bonterra is a recipient of Covered Data in the United States. Bonterra has certified to the Data Privacy Framework. Customer authorizes Bonterra to perform transfers of Covered Data out of the EEA, Switzerland, or the United Kingdom to the U.S. based on Bonterra's certification. The parties agree that the Data Privacy Framework is the primary mechanism for data transfers to the U.S. If Bonterra withdraws from the Data Privacy Framework, the Data Privacy Framework is invalidated, or otherwise Covered Data cannot be lawfully received based on the Data Privacy Framework, the International Data Transfer Terms listed on in Section 2 of this Appendix) above will automatically apply.

4. Standard Contractual Clauses (EU)

Where EU GDPR applies to Customer's transfer, the parties enter into Module Two (Controller-to-Processor) of the SCCs, which are incorporated by reference and completed as follows:

(a) Clause 7 (docking clause): applies.

(b) Clause 9(a): Option 2 applies. The prior notice period for Subprocessor changes is 30 days, satisfied by Bonterra's Trust Center update process in Section 8 of this DPA.

(c) Clause 11 (independent dispute resolution): does not apply.

(d) Clause 17: Option 1 applies; governing law is the law of the Republic of Ireland.

(e) Clause 18(b): disputes are resolved before the courts of the Republic of Ireland.

(f) Annex I to the SCCs is Annex I of this DPA.

(g) Annex II to the SCCs is Annex II of this DPA.

(h) Annex III to the SCCs is the Subprocessor list published on Bonterra's Trust Center.

5. UK Addendum

In relation to Personal Data protected by UK GDPR, the EU SCCs completed as set out in Section 4 of this Appendix will also apply to transfers of such Personal Data, subject to the following:

5.1. The UK Addendum, issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, will be deemed executed between Customer and Bonterra upon execution of this DPA, and the EU SCCs will be deemed amended as specified by the UK Addendum in respect of the transfer of such Personal Data.

5.2. If the UK Addendum cannot be relied upon for a given transfer, Customer and Bonterra will cooperate in good faith to implement appropriate safeguards for that transfer as required or permitted by UK GDPR without undue delay.

6. Swiss Addendum

Where Swiss data protection law (including the Federal Act on Data Protection - "FADP") applies, the SCCs apply with the following modifications: (a) references to "Regulation (EU) 2016/679" are replaced with the applicable Swiss data protection law; (b) references to "EU," "Union," and "Member States" are replaced with "Switzerland"; (c) Clause 13 and the competent supervisory authority are replaced with the Swiss Federal Data Protection and Information Commissioner (FDPIC); (d) Clause 17 is replaced to state governing law is Swiss law; and (e) Clause 18 is replaced to state disputes are resolved before Swiss courts.

7. Security of Processing Assistance

Bonterra will provide reasonable assistance to Customer to fulfill Customer's obligations under Articles 32-36 of the GDPR (security, breach notification, data protection impact assessments, and prior consultation), to the extent the relevant information is in Bonterra's possession and not otherwise accessible to Customer.

8. Records of Processing

Bonterra will maintain records of processing activities as required by Article 30(2) of the GDPR and will make those records available to a supervisory authority on request.

9. Right to Compensation and Liability

Where a Data Subject asserts any claims against Bonterra in accordance with Article 82 of GDPR, Customer will immediately notify Bonterra in writing and will support Bonterra in defending against such claims.

10. Subprocessors

Customer may object in writing to the appointment of a Subprocessor with legitimate reasons relating to the protection of Covered Data under GDPR within 10 days after the notice was posted by Bonterra in writing. If

no such written refusal has been made, consent will be deemed granted. If Customer objects the appointment of a Subprocessor as set forth herein, Customer and Bonterra will work together in good faith to achieve a mutually agreeable solution. In addition, Bonterra will have the right in its sole discretion to stop using that Subprocessor for its engagement with Customer, and appoint a new Subprocessor, or suspend or terminate the affected Service. Authorizations under Section 8 of this DPA will also constitute Customer's prior written consent to Bonterra's use of Subprocessors if such consent is required under Standard Contractual Clauses.

11. SCC Conflicts

In the event of a conflict between any provision of this DPA and the SCCs, the SCCs prevail for any Restricted Transfer.

ANNEX I

Processing Details

A. List of Parties

	Data Exporter (Customer)	Data Importer (Bonterra)
Role	Controller	Processor
Contact/Address	Identified on the Principal Agreement	Identified in the Principal Agreement
Signature	Deemed executed upon signing the DPA	Deemed executed upon execution of the Principal Agreement

B. Description of Processing

Activities relevant to the data transferred	Bonterra's provision of the Bonterra Products to Customer as listed on the Principal Agreement (including an Order Form or SOW).
Duration	For the term of the Principal Agreement, unless earlier termination is agreed.
Nature and Purpose	Processing necessary to deliver, maintain and support the Bonterra products licensed to Customer.
Frequency	Continuous.
Categories of Data	Data relating to individuals provided by or on behalf of Customer, which may include: (a) First and last name (b) E-mail and mailing address (c) IP address and device identifiers (d) Employment data (for applicable products) (e) Any other categories Customer submits through the licensed Bonterra product (f) Access credentials (username, password) (g) Transactional data (payments, transactions and purchases made by users through the licensed Bonterra product) (h) Platform activity data, such as details about donations and participation in social impact events (e.g. projects initiated / participated in, charities donated to, comments, opinions and engagement on social impact projects and donations campaigns)

	(i) Preference data (*e.g.*, profile/account settings, interest in specific topics, etc.) (j) Support requests
Special Categories	Not intended for processing unless agreed in a signed amendment to this Annex.
Data Subjects	Customer's authorized users, employees, contractors, affiliates, end users, donors, volunteers, and individuals whose data Customer submits through licensed Bonterra product.

C. Competent Supervisory Authority

Where EU GDPR applies: Irish Data Protection Commission (or the supervisory authority of Customer's EU establishment if different).

Where UK GDPR applies: UK Information Commissioner's Office.

Where Swiss law applies: Swiss Federal Data Protection and Information Commissioner (FDPIC).

Annex II

Technical and Organizational Security Measures

Bonterra maintains a comprehensive, written information security program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of Bonterra's business; (b) the type of information that Bonterra will store; and (c) the need for security and confidentiality of such information. These include:

Security Awareness and Training. A mandatory security awareness and training program for all members of Bonterra's workforce (including management), which includes training on how to implement and comply with its Information Security Program and promoting a culture of security awareness through periodic communications from senior management.

Access Controls. Policies, procedures, and logical controls to limit access to its information systems to properly authorized persons, prevent unauthorized access, and remove access in a timely basis in the event of a change in job responsibilities or status.

Physical and Environmental Security. Controls that provide reasonable assurance that access to physical servers at the production data center is limited to properly authorized individuals, including logging and monitoring of unauthorized access attempts, camera surveillance systems, environmental monitoring, and redundant power supply modules and backup generators.

Personal Data Breach Procedures. A security incident response plan that includes procedures to be followed in the event of any Personal Data Breach, including defined roles and responsibilities, investigation procedures, communication protocols, recordkeeping, and root cause analysis.

Contingency Planning. Policies and procedures for responding to emergencies or other occurrences that could damage Covered Data, including data backup policies, a formal disaster recovery plan tested at least annually, and a business continuity plan.

Audit Controls. Hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use Covered Data.

Data Integrity. Policies and procedures to ensure the confidentiality, integrity, and availability of Covered Data and protect it from disclosure, improper alteration, or destruction.

Storage and Transmission Security. Security measures to guard against unauthorized access to Covered Data being transmitted over a public electronic communications network or stored electronically, including requiring AES 128-bit or stronger encryption.

Secure Disposal. Policies and procedures regarding the secure disposal of tangible property containing Covered Data, using methods that render data unrecoverable.

Assigned Security Responsibility. A designated security official with overall responsibility, defined security roles, and a Security Council of cross-functional management representatives.

Testing. Regular testing of key controls, systems, and procedures, including internal risk assessments, ISO 27001 and ISO 27018 certifications, and SOC 2 Type 2 audit reports.

Monitoring. Network and systems monitoring including error logs, review of privileged access, and regular third-party network vulnerability assessments and penetration testing.

Change and Configuration Management. Policies and procedures for managing changes to production systems, applications, and databases, including a security patching process and application-level security assessments.

Devices. All laptop and desktop computing devices used by Bonterra and subcontractors when accessing Covered Data will be equipped with AES 128-bit full disk encryption and up-to-date virus and malware detection software.

Appendix B

Additional Terms: United States

These additional terms apply to Covered Data processed in connection with Customer's activities in the United States. Capitalized terms not defined here have the meanings given in the main DPA.

B.1 Definitions

"CCPA" means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act of 2020, and its implementing regulations.

"Business," "Service Provider," "Sell," and "Share" have the meanings given in the CCPA.

B.2 Roles

For purposes of the CCPA and other applicable U.S. state privacy laws, Customer is a Business and Bonterra is a Service Provider with respect to Covered Data.

B.3 CCPA Certification

Bonterra certifies that it will not:

(a) "Sell" or "Share" Covered Data as those terms are defined under the CCPA;

(b) retain, use, or disclose Covered Data for any commercial purpose other than providing the services; or

(c) combine Covered Data with personal information collected from or on behalf of other businesses, or from Bonterra's own interactions with individuals, except as permitted under the CCPA.

B.4 Other U.S. State Privacy Laws

To the extent other U.S. state privacy laws apply to the processing of Covered Data, Bonterra will process Covered Data consistent with its role as a service provider or processor under those laws, and will comply with obligations substantially equivalent to those in Section B.3 of this Appendix.