DATA PROCESSING ADDENDUM

Bonterra LLC ("**Bonterra**") is an online, cloud-based service platform that includes EveryAction, CyberGrants, Network for Good, Social Solutions and the respective individualized service offerings thereunder. This Data Processing Addendum ("**DPA**") amends and forms part of the written agreement between **Customer** and **Bonterra** (collectively, "**the parties**") for the provision of services to Customer (the "**Agreement**"). This DPA prevails over any conflicting term of the Agreement but does not otherwise modify the Agreement.

1. **Definitions**

1.1. In this DPA:

a) "**Controller**", "**Data Subject**", "**Processing**", "**Processor**", "**Service Provider**", and "**Supervisory Authority**" have the meaning given to them in Data Protection Law (as defined below);

b) "**Data Protection Law**" means the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and all other Data Protection Laws of the European Union, the European Economic Area ("**EEA**"), and their respective Member States, Switzerland and the United Kingdom ("**UK**"); (ii) certain U.S. federal and state privacy laws, including the California Consumer Protection Act (California Civil Code § 1798.100) ("**CCPA**"); and (iii) all laws implementing or supplementing the foregoing;

c) "**Data Subject Rights**" means all rights granted to Data Subjects by Data Protection Law, such as the right to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to automated individual decision-making;

d) "**Restricted Data Transfer**" means any international transfer of Personal Data that would be prohibited under Data Protection Law in the EEA or UK without implementation of additional safeguards such as Standard Contractual Clauses.

e) "**Personnel**" means any natural person acting under the authority of Bonterra;

f) "**Personal Data**" means any information that constitutes "personal data" or "personal information" within the meaning of applicable Data Protection Law that Bonterra may access in performing the services under the Agreement.

g) "**Personal Data Breach**" means actual or reasonable degree of certainty of unauthorized destruction, loss, control, alteration, disclosure of, or access to, Personal Data for which Bonterra is responsible. Personal Data Breaches do not include unsuccessful access attempts or attacks that do not compromise the confidentiality, integrity, or availability of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

h) "**Sensitive Data**" means any type of Personal Data that is designated as a sensitive or special category of Personal Data, or otherwise subject to additional restrictions under Data Protection Law or other laws to which the Controller is subject;

i) "**Subprocessor**" means a Processor engaged by a Processor to carry out Processing on behalf of a Controller;

j) "**Standard Contractual Clauses**" means the clauses annexed to the EU Commission Implementing Decision 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council as amended or replaced from time to time; and

k) **"UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK Information Commissioner for parties making restricted transfers.

1.2. Capitalized terms used but not defined herein have the meaning given to them in the Agreement.

2. **Roles**

2.1. If Data Protection Law applies to the Processing of Personal Data, the parties agree that Bonterra shall process Personal Data only as a Processor acting on behalf of Customer and, with respect to CCPA and other applicable U.S. state privacy laws, as a service provider, in each case, regardless of whether Customer acts as a Controller or as a Processor on behalf of a third-party Controller with respect to Personal Data.

3. **Scope**

3.1. This DPA applies to Processing of Personal Data by Bonterra in the context of the Agreement.

3.2. The subject matter, nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set out in **Annex I**, which is an integral part of this DPA.

4. **Instructions**

4.1. Bonterra will only Process Personal Data to provide the services to Customer.

4.2. It is the parties' intent that Bonterra is a Service Provider, and Bonterra certifies that it will not (a) "sell" (as defined in the CCPA) the Personal Data; (b) retain, use, or disclose the Personal Data for any purpose other than for the specific purpose of providing the services under the Agreement, including retaining, using, or disclosing the personal information for a commercial purpose other than the provision of the services; or (c) retain, use, or disclose the Personal Data to any person other than as necessary to provide the services or outside of the direct business relationship between the parties.

4.3. Customer's instructions are documented in **Annex I**, the Agreement, and any applicable statement of work.

4.4. Customer may issue additional instructions to Bonterra as it deems necessary to comply with Data Protection Law. Such instructions must be provided to Bonterra in writing and acknowledged in writing by Bonterra as constituting instructions for purposes of this DPA, and Bonterra may charge a reasonable fee to comply with any such additional instructions.

5. **Customer Responsibilities**

5.1 Customer is responsible for the lawfulness of Personal Data processing under or in connection with the services. Customer shall (i) have provided, and will continue to provide all notices and have obtained, and will continue to obtain, all consents, permissions and rights necessary under applicable Data Protection Law for Bonterra to lawfully process Personal Data for the purposes contemplated by the Agreement (including this DPA); (ii) make appropriate use of the services to ensure a level of security appropriate to the particular content of the Personal Data; (iii) have complied with all Data Protection Law applicable to the collection of Personal Data and the transfer of such Personal Data to Bonterra and its Subprocessors; and (iv) ensure its processing instructions comply with applicable laws (including applicable Data Protection Law).

6. **Subprocessing**

6.1. Bonterra will provide to Customer prior written notice to engage Subprocessors. Customer hereby authorizes Bonterra to engage the Subprocessors listed in **Annex III**.

6.2. Bonterra will inform Customer at least thirty (30) days prior to any intended change of Subprocessor, thereby giving Customer the opportunity to object to such change. Customer may only object to the addition of a Subprocessor based on reasonable grounds relating to a potential or actual violation of Data Protection Law by providing written notice detailing the grounds of such objection. Customer and Bonterra will work together in good faith to address Customer's objection.

6.3. Bonterra will enter into a written agreement with all Subprocessors which imposes substantially similar obligations on the Subprocessors as this DPA imposes on Bonterra.

6.5 To the extent required by law, Bonterra will provide a copy of Bonterra's agreements with Subprocessors to Customer upon request. Bonterra may redact commercially sensitive information before providing such agreements to Customer.

7. **Restricted Data Transfers**

7.1. To the extent required by Data Protection Law in the EEA, by agreeing to this DPA Customer and Bonterra conclude module 2 (Controller-to-Processor) of the Standard Contractual Clauses, which are hereby incorporated by reference and completed as follows: the "data exporter" is Customer; the "data importer" is Bonterra; the optional docking clause in Clause 7 is implemented; Clause 9(a) option 1 is implemented and the time period therein is specified as thirty (30) days; the optional redress clause in Clause 11(a) is struck; Clause 13, (a) paragraph 2 is implemented; Clause 17 option 1 is implemented and the governing law is the law of the Republic of Ireland; the court in Clause 18(b) are the Courts of the Republic of Ireland; Annex 1, 2 and 3 to module 2 of the Standard Contractual Clauses are **Annex I, II** and **III** to this DPA respectively.

7.2. To the extent required by Data Protection Law in the UK, by signing this DPA Customer and Bonterra agree to be bound by the UK Addendum. Part 1, table 1 of the UK Addendum will be deemed to be completed like its equivalent provisions in the Standard Contractual Clauses (module 2) in Annex I, Section 1. For the purpose of Part 1, Table 2 of the UK Addendum, the Approved EU SCCs are the Standard Contractual Clauses (module 2) incorporated by reference into this DPA pursuant to Section 7.1 of this DPA. For the purpose of Part 1, Table 3, Annex 1, 2 and 3 to the Standard Contractual Clauses (module 2) are **Annex I, II** and **III** to this DPA respectively. For the purpose of Part 1, Table 4, the party that may end the UK Addendum in accordance with Section 19 of the UK Addendum is the importer. For the purposes of any transfers covered by the Data Protection Law in the UK, the Standard Contractual Clauses (module 2) will be deemed to be amended as set out in Part 2 of the UK Addendum.

8. **Personnel**

8.1. Bonterra will take steps to ensure that all Personnel authorized to Process Personal Data agree to appropriate confidentiality arrangements.

8.2. Bonterra will train Personnel regarding the protection of Personal Data.

9. **Security and Personal Data Breaches**

9.1. Bonterra will implement technical and organizational measures to protect Personal Data from Personal Data Breaches, such as:

a) encryption of Personal Data;

b) measures to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing;

c) measures to detect Personal Data Breaches in a timely manner;

d) measures to restore the availability and access to Personal Data in a timely manner in the event of an incident;

e) Processes for regularly testing, assessing and evaluating the effectiveness of the security measures; and

f) as appropriate, the measures listed in **Annex II**.

9.2. Bonterra will inform Customer without undue delay and no later than one (1) business day after becoming aware of a Personal Data Breach. Bonterra will inform Customer to the extent possible, of the nature of the Personal Data Breach, the categories and number of Data Subjects, the categories and amount of Personal Data, the likely consequences of the Personal Data Breach, and the measures taken or proposed to be taken to address the Personal Data Breach and mitigate possible adverse effects.

9.3. Bonterra's notification of or response to a Personal Data Breach under Section 9.2 will not be construed as an acknowledgement by Bonterra of any fault or liability with respect to the Personal Data Breach.

10. **Assistance**

10.1. Bonterra will reasonably assist Customer, including by implementing appropriate technical and organizational measures, with the fulfilment of Customer's own obligations under Data Protection Law, including:

a) complying with Data Subjects' requests to exercise Data Subject Rights;

b) replying to inquiries or complaints from Data Subjects;

c) replying to investigations and inquiries from Supervisory Authorities;

d) conducting data protection impact assessments, and prior consultations with Supervisory Authorities; and

e) notifying Personal Data Breaches.

10.2. Unless prohibited by Data Protection Law, Bonterra will inform Customer if Bonterra:

a) receives a request, complaint or other inquiry regarding the Processing of Personal Data from a Data Subject or Supervisory Authority;

b) receives a binding or non-binding request to disclose Personal Data from law enforcement, courts or any government body;

c) is subject to a legal obligation that requires Bonterra to Process Personal Data in contravention of Customer's instructions; or

d) is otherwise unable to comply with Data Protection Law or this DPA.

10.3. Unless prohibited by Data Protection Law, Bonterra will obtain Customer's written authorization before responding to, or complying with any requests, orders, or legal obligations referred to in Section 10.2.

11. **Accountability**

11.1. Bonterra will maintain records of all Processing of Personal Data, including at a minimum the categories of information required under Data Protection Law, and will provide a copy of such records to Customer upon request.

11.2. Bonterra will inform Customer without undue delay if Bonterra believes that a written instruction amending this DPA by Customer violates Data Protection Law, in which case Bonterra may suspend the Processing until Customer has modified or confirmed the lawfulness of the instructions in writing.

12. **Audit**

12.1. Upon Customer's prior written request, and no more than once in a calendar year, Bonterra will make available to Customer the required information reasonably necessary to demonstrate compliance with the obligations of Data Protection Law and this DPA. Bonterra shall provide additional information as reasonably necessary to allow for and contribute to audits, including inspections, conducted by a Supervisory Authority, Customer or another auditor mandated by law.

12.2. If a third party is to conduct the audit, Bonterra may object to the auditor if the auditor is, in Bonterra's reasonable opinion, not suitably qualified or independent, a competitor of Bonterra or otherwise manifestly unsuitable. Such objection by Bonterra will require Customer to appoint another auditor or conduct the audit itself.

12.3. The audit must be conducted during regular business hours at the applicable facility, subject to an audit plan agreed to between the parties at least two weeks in advance and Bonterra's health and safety or other relevant policies and may not unreasonably interfere with Bonterra's business activities.

12.4. If Customer's requested audit scope is addressed in an SSAE 16/ISAE 3402 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request and Bonterra confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

12.5. Any Customer-requested audits are at Customer's expense. Customer shall reimburse Bonterra for any time expended by Bonterra or its Subprocessors in connection with any Customer-requested audits or inspections at Bonterra's then-current professional services rates, which shall be made available to Customer upon request.

12.6. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA. The audit reports are confidential information of the parties under the terms of the Agreement.

13. **Liability**

13.1. The total combined liability of either party and its Affiliates towards the other party and its Affiliates, whether in contract, tort or any other theory of liability, under or in connection with Agreement and this DPA combined, will be limited to limitations on liability or other liability caps agreed to by the parties in the Agreement.

14. **Confidentiality**

14.1. Bonterra will keep all Personal Data and all information relating to the Processing thereof, in strict confidence.

15. **Analytics**

15.1 Customer acknowledges and agrees that Bonterra may create and derive from Processing related to the services anonymized and/or aggregated data that does not identify Customer or any natural person, and use, publicize or share with third parties such data to improve Bonterra's products and services and for its other legitimate business purposes.

16. **Notifications**

16.1. Bonterra will make all notifications required under this DPA as agreed to in the Agreement or the then established daily point of contact with the Customer.

17. **Term and Duration of Processing**

17.1. The Processing will last no longer than the term of the Agreement.

17.2. Upon termination of the Processing, Bonterra will, at Customer's choice, delete or return all Personal Data and will delete all remaining copies within ninety (90) days after confirmation of Customer's choice (or earlier as agreed to between the parties).

17.3. This DPA is terminated upon Bonterra's deletion of all remaining copies of Personal Data in accordance with Section 17.2.

18. **Modification of this DPA**

18.1. This DPA may only be modified by a written amendment signed by both Customer and Bonterra.

19. **Invalidity and Severability**

19.1. If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

Accepted and agreed to by the authorized representative of each party:

Customer	**Bonterra**
_____	_____
Authorized Signature	Authorized Signature
_____	_____
Name	Name
_____	_____
Title	Title
_____	_____
Date	Date

ANNEX I

A. LIST OF PARTIES

Customer is the Controller and the data exporter and Bonterra is the Processor and the data importer.

B. DESCRIPTION OF TRANSFER

Subject Matter	Bonterra's provision of the services to Customer.
Duration of the Processing	For the term of the Agreement and as required under applicable law.
Nature and Purpose of the Processing	Bonterra will process Customer Personal Data for the purposes of providing the services to Customer in accordance with the DPA.
Frequency of the Processing	Continuous.
Categories of Data	Data relating to individuals provided to Bonterra in connection with the services, by (or at the direction of) Customer. The minimum Personal Data necessary to use the services are: first and last name, electronic mailing address, mailing address, and an Internet Protocol (IP) address from the electronic device.
Sensitive Data Processed	The services are not intended to Process special categories of data unless otherwise agreed to in a signed amendment to this Annex.
Data Subjects	Customers' authorized users of the services which include Customer's employees, contractors and affiliates, as well as users of charitable, political, and tax exempt organizations authorized by Customer to access the services.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority is the Irish Data Protection Commission.

ANNEX II

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.

Bonterra's security program includes:

1. **Security Awareness and Training**. A mandatory security awareness and training program for all members of Bonterra's workforce (including management), which includes:
    a. Training on how to implement and comply with its Information Security Program; and
    b. Promoting a culture of security awareness through periodic communications from senior management with employees.
2. **Access Controls**. Policies, procedures, and logical controls:
    a. To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;
    b. To prevent those workforce members and others who should not have access from obtaining access; and
    c. To remove access in a timely basis in the event of a change in job responsibilities or job status.
3. **Physical and Environmental Security**. Controls that provide reasonable assurance that access to physical servers at the production data center, if applicable, is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes.
    a. Logging and monitoring of unauthorized access attempts to the data center by the data center security personnel;
    b. Camera surveillance systems at critical internal and external entry points to the data center, with retention of data per legal or compliance requirements;
    c. Systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and
    d. Redundant power supply modules and backup generators that provide backup power in the event of an electrical failure, 24 hours a day.
4. **Personal Data Breach Procedures**. A security incident response plan that includes procedures to be followed in the event of any Personal Data Breach. Such procedures include:
    a. Roles and responsibilities: formation of an internal incident response team with a response leader;
    b. Investigation: assessing the risk the incident poses and determining who may be affected;
    c. Communication: internal reporting as well as a notification process in the event of unauthorized disclosure of Personal Data;
    d. Recordkeeping: keeping a record of what was done and by whom to help in later analysis and possible legal action; and
    e. Audit: conducting and documenting root cause analysis and remediation plan.
5. **Contingency Planning**. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Personal Data or production systems that contain Personal Data. Such procedures include:
    a. Data Backups: A policy for performing periodic backups of production data sources, as applicable, according to a defined schedule;
    b. Disaster Recovery: A formal disaster recovery plan for the production data center, including:
        i. Requirements for the disaster plan to be tested on a regular basis, currently annually; and

ii. A documented executive summary of the Disaster Recovery testing, at least annually, which is available upon request to customers.

c. Business Continuity Plan: A formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

6. **Audit Controls**. Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information.

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

8. **Storage and Transmission Security**. Security measures to guard against unauthorized access to Personal Data that is being transmitted over a public electronic communications network or stored electronically. Such measures include requiring encryption of any Personal Data stored on desktops, laptops or other removable storage devices.

9. **Secure Disposal**. Policies and procedures regarding the secure disposal of tangible property containing Personal Data, taking into account available technology so that Personal Data cannot be practicably read or reconstructed.

10. **Assigned Security Responsibility**. Assigning responsibility for the development, implementation, and maintenance of Bonterra's security program, including:

    a. Designating a security official with overall responsibility;

    b. Defining security roles and responsibilities for individuals with security responsibilities; and

    c. Designating a Security Council consisting of cross-functional management representatives to meet on a regular basis.

11. **Testing**. Regularly testing the key controls, systems and procedures of its information security program to validate that they are properly implemented and effective in addressing the threats and risks identified. Where applicable, such testing includes:

    a. Internal risk assessments;

    b. ISO 27001 and ISO 27018 certifications; and

    c. Service Organization Control 2 (SOC2) audit reports (or industry-standard successor reports).

12. **Monitoring**. Network and systems monitoring, including error logs on servers, disks and security events for any potential problems. Such monitoring includes:

    a. Reviewing changes affecting systems handling authentication, authorization, and auditing;

    b. Reviewing privileged access to Bonterra production systems; and

    c. Engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

13. **Change and Configuration Management**. Maintaining policies and procedures for managing changes Bonterra makes to production systems, applications, and databases. Such policies and procedures include:

    a. Process for documenting, testing and approving the patching and maintenance of the Bonterra Product;

    b. A security patching process that requires patching systems in a timely manner based on a risk analysis; and

    c. A process for Bonterra to utilize a third party to conduct application-level security assessments. These assessments generally include testing, where applicable, for:

        i. Cross-site request forgery

        ii. Services scanning

        iii. Improper input handling (e.g. cross-site scripting, SQL injection, XML injection, cross-site flashing)

        iv. XML and SOAP attacks

v. Weak session management

vi. Data validation flaws and data model constraint inconsistencies

vii. Insufficient authentication

viii. Insufficient authorization

14. **Program Adjustments**. Monitoring, evaluating, and adjusting, as appropriate, the security program in light of:

    a. Any relevant changes in technology and any internal or external threats to Bonterra or the Personal Data;

    b. Security and data privacy regulations applicable to Bonterra; and

    c. Bonterra's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

15. **Devices** – Ensuring that all laptop and desktop computing devices utilized by Bonterra and any subcontractors when accessing Personal Data:

    a. Will be equipped with a minimum of AES 128 bit full hard disk drive encryption;

    b. Will have up to date virus and malware detection and prevention software installed with virus definitions updated on a regular basis; and

    c. Will maintain virus and malware detection and prevention software so as to remain on a supported release. This will include, but not be limited to, promptly implementing any applicable security-related enhancement or fix made available by the supplier of such software.

ANNEX III

List of Subprocessors

Customer authorizes Bonterra to engage the following Subprocessors:

Bonterra maintains an up-to-date list of name and locations of all sub-processors. Customers can obtain a copy by contacting legal@bonterratech.com.