Data Processing Agreement ("Agreement")

Unless otherwise defined below, all capitalised terms used in this Agreement will have the meanings given to them under the Terms of Service.

WHEREAS

(A) Pursuant to Section 4.3 of the Terms, you (the "**Controller**") have appointed Impact Track (the "**Processor**") to provide the Services via the Platform. In performing its obligations under the Terms, the Processor will collect and process Impact Personal Data on behalf of the Controller.

(B) The Controller will remain the Controller with regard to the processing of Impact Personal Data and the Processor does not have any independent control over the Impact Personal Data to be processed by the Processor on behalf of the Controller.

(C) This Agreement is being put in place to ensure that the Processor collects and processes Impact Personal Data on behalf of the Controller in accordance with the Controller's instructions, this Agreement and in compliance with all applicable data protection laws, including the GDRP ("**Data Protection Laws**").

THE FOLLOWING IS HEREBY AGREED:

1. Definitions

1.1 For the purposes of this Agreement, the following expressions bear the following meaning:

(a) "**Agreement**" means this data processing agreement including its appendix;

(b) "**Authority**" means the French Data Protection Authority (the CNIL and any successors);

(c) "**Data Subject Requests**" means request(s) of data subject(s) to access, rectify, change, delete or port personal data or to restrict or object to the processing of personal data, or any other rights granted to data subjects under the GDPR;

(d) "**Effective Date**" means the date when you accept the Terms in accordance with Section 2.2 of the Terms;

(e) "**Security Breach**" means all actual or suspected personal data breaches, unauthorized access, loss, misuse, damage or any other breach of the security, confidentiality or integrity of the personal data processed by the Processor or its sub-processor(s) on behalf of the Controller.

1.2 In this Agreement, the terms "data subject", "personal data", "process/processing", "personal data breach" and "data protection impact assessment" are as defined in the GDPR.

2. SCOPE OF THE PROCESSING

The details of processing carried out by the Processor are set out in **Appendix 1**.

3. TERM OF THE AGREEMENT

This Agreement will take effect from the Effective Date of the Terms and remain in force until, and automatically expire upon, deletion of all Impact Personal Data by the Processor, unless instructed otherwise by the Controller.

4. CONTROLLER'S OBLIGATIONS

4.1 The Controller shall obtain and maintain any required consents necessary to permit the collection and the processing of Impact Personal Data and comply with any other obligations under all applicable Data Protection Laws with regard to the processing of Impact Personal Data.

4.2 The Controller acknowledges that it is solely responsible for determining the adequacy of the security measures in relation to the processing of Impact Personal Data.

5. PROCESSOR'S OBLIGATIONS

5.1 Instructions and advice

The Processor shall:

(a) act only on documented instructions and directions from the Controller, which the Controller may change at any time, and in accordance with the terms of this Agreement. The Controller may at any time suspend the processing by the Processor;

(b) only process the personal data for the purpose of carrying out the Services and not process the personal data for its own purposes without the prior written consent of the Controller;

(c) maintain a record of its processing activities under this Agreement and make it available to the Authority on request in compliance with Article 30 of the GDPR; and

(d) abide by any specific advice of authorities addressed to the Processor with regard to the processing of Impact Personal Data, subject to prior notification to the Controller.

The Processor will have no liability for any harm or damages resulting from its compliance with the instructions received from the Controller.

5.2 Notification

Unless the Processor is prohibited from doing so (in which case the Processor shall inform the Authority and comply with the instructions given by the Authority), the Processor shall immediately notify the Controller or its European representative when:

(a) it becomes aware of any Security Breach;

(b) it receives a request for disclosure of personal data;

(c) applicable law to which it is subject requires it to process the personal data other than in accordance with the Controller's instructions and this Agreement;

(d) it is of the opinion that an instruction from the Controller violates the Data Protection Laws, this Agreement or any other applicable law to which it is subject; or

(e) it receives a complaint, request or other communication of a data subject or the Authority, including Data Subject Requests, without responding to the complaint, request or communication.

5.3 Assistance and cooperation

The Processor will provide reasonable assistance and cooperate with the Controller in complying with the Controller's obligations under applicable Data Protection Laws, notably including the obligations:

(a) in relation to investigating, restoring and promptly notifying the Authority and/or data subjects of personal data breaches;

(b) to carry out data protection impact assessments or audits of the processing activities carried out by the Processor on behalf of the Controller;

(c) to respond to Data Subject Requests and complaints and requests from the Authority; and

(d) to consult with the Authority prior to the processing in relation to processing activities subject to data protection impact assessments.

In any event, the Controller is solely responsible for carrying out its obligations in accordance with Data Protection Laws.

5.4 Processor personnel

The Processor guarantees that all persons with access to the Impact Personal Data, or otherwise involved in the processing of Impact Personal Data, on behalf of or as instructed by the Processor, are made aware of the Controller's instructions and the confidentiality of Impact Personal Data. In this regard, the Processor will:

(a) take reasonable steps to ensure the reliability of all these persons;

(b) ensure that all these persons have signed a confidentiality agreement or are under an appropriate statutory obligation of confidentiality;

(c) ensure that all these persons will keep the Impact Personal Data confidential after termination of this Agreement and/or after completion of the processing activities;

(d) ensure that none of these persons will process the Impact Personal Data except under instructions from the Controller; and

(e) provide necessary training to these persons with respect to their obligations under this Agreement and Data Protection Laws, and ensure that these persons are aware of and comply with such obligations.

5.5 Data security measures

The Processor will:

(a) not disclose the Impact Personal Data to any third party unless (a) it is strictly necessary for the performance of the Services, (b) it is necessary to comply with applicable law to which it is subject, or (c) the Controller has provided prior written consent;

(b) not process the Impact Personal Data outside of IT systems determined by the Controller and will use any technical security measures put in place by the Controller to secure the Impact Personal Data;

(c) implement and maintain all appropriate organizational and technical measures:

(i) to protect the security and confidentiality of the Impact Personal Data processed by the Processor in connection with the Services; and

(ii) to protect the Impact Personal Data against accidental or unlawful processing, including destruction or loss, alteration, unauthorized disclosure or access,

taking into account the nature of any risks and the level of damage and/or distress that a data subject might suffer from any breach of confidentiality or

accidental or unlawful processing. These measures shall include the security measures agreed upon by the Parties in **Appendix 2**.

(d) without undue delay, notify the Controller of a Security Breach and cooperate with the Controller in handling and managing any reasonable obligations which may apply to the Controller further to a Security Breach.

6. **DATA SUBJECT RIGHTS**

6.1 The Processor will put in place appropriate technical and organizational measures to assist the Controller in complying with its obligations to respond to Data Subject Requests.

6.2 The Processor will immediately notify the Controller of any Data Subject Request received directly from the data subject. The Controller will be solely responsible for responding to any Data Subject Requests forwarded by the Processor.

7. **AUDITS**

7.1 The Processor will make available to the Controller all information necessary to demonstrate the Processor's compliance with the obligations laid down in this Agreement.

7.2 The Processor shall authorize and contribute to audits, including inspections by the Controller or another auditor mandated by the Controller. Such audits may be conducted at reasonable intervals (i.e. no more than once per year), with a prior notice of at least thirty (30) days. The Controller shall bear the costs of such audits.

8. **SUB-PROCESSING**

8.1 The Controller authorizes the Processor to engage sub-processors to fulfill its obligations under this Agreement. The information about these sub-processors is available at https://www.impacttrack.org/en/legal-information/.

8.2 When engaging any sub-processor, the Processor will ensure via a written contract requiring that the sub-processor abide by the same obligations under the Agreement.

8.3 The Processor remains fully liable for all obligations subcontracted to, and all acts and omissions of, the sub-processor.

8.4 The Controller may object to the Processor's proposed use of a new sub-processor by notifying the Processor in writing within ten (10) days from receipt of the Processor's written notice specifying the name of the relevant sub-processor and the activities it will perform. The Processor shall notify the Controller within thirty (30) days from receipt of the Controller's objection notice of its final decision regarding the use of the sub-processor at issue. The Controller may terminate its subscription upon written notice to the Processor within fifteen (15) days from receipt of the Processor's

notification of its intention to engage the sub-processor at issue and, as the Controller's sole and exclusive remedy, the Processor will refund the Controller, *pro rata*, the prepaid subscription fees covering the remainder of the Services specified in the related order form after the effective date of the termination.

9. DATA TRANSFERS

9.1 If the storage and/or processing of Impact Personal Data by the Processor involves transfers of such data to a sub-processor established in a country outside of the European Economic Area (EEA) without an adequate level of protection, the Processor will ensure that the sub-processor at issue abide by any lawful mechanism for the data transfer as approved by the European Commission, including but not limited to the EU Standard Contractual Clauses and the EU-US privacy shield framework.

9.2 A list of transfers for which the Controller grants its authorisation upon the conclusion of the Terms and of this Agreement is available at https://www.impacttrack.org/en/legal-information/. The Processor shall promptly notify the Controller of any planned permanent or temporary transfers outside of the EEA, which may be refused by the Controller in accordance with Section 8.4 of the Agreement.

10. LIABILITY

The total combined liability of either party under the Agreement will be limited to the liability cap set forth in Section 14.2 of the Terms.

11. DELETION OF IMPACT PERSONAL DATA

11.1 Upon termination or expiration of the Controller's subscription of the Services, the Controller will continue to have the ability to retrieve the Impact Personal Data within thirty (30) days following the effective date of termination or expiration. After that 30-day period, the Processor will delete all Impact Personal Data, unless prohibited by laws, court orders or regulatory requirements.

11.2 If the Processor cannot delete or return the Impact Personal Data due to legal or regulatory requirements, the Processor will immediately inform the Controller and will take all necessary steps to ensure that the Impact Personal Data concerned is kept confidential and will not be further processed.

12. GOVERNING LAW AND JURISDICTION

12.1 This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) will be governed by the law of France.

12.2 The Parties irrevocably agree that the courts of Paris will have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims).

Appendix 1

Details of data processing

NATURE AND PURPOSE OF PROCESSING

The Processor will process Impact Personal Data for the purpose of providing the Services in accordance with the Terms.

DATA SUBJECTS

Data subjects include the individuals whose personal data is collected by the Processor on behalf of the Controller via the Platform or directly submitted by the Controller to the Services.

CATEGORIES OF PERSONAL DATA

The categories of Impact Personal Data will be solely determined by the Controller.

SPECIAL CATEGORIES OF PERSONAL DATA

Special categories of personal data may be collected and processed by the Processor as instructed by the Controller, the extent of which will be solely determined by the Controller in compliance with Data Protection Laws.

DURATION OF THE PROCESSING

The Processor will process the Impact Personal Data for the time necessary to provide the Services in accordance with the Terms and the Controller's instructions, unless otherwise required by applicable laws.

PROCESSING OPERATIONS

All activities necessary for the performance of the Agreement, which may include but not limited to collection, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

SUB-PROCESSORS AND DATA TRANSFERS

The list of transfers to sub-processors in third countries, including countries outside the EEA without an adequate level of protection, is available at https://www.impacttrack.org/en/legal-information/.

Appendix 2

Security Measures

The Processor shall:

1. ensure that the Impact Personal Data can be accessed only by authorized personnel for the purposes set forth in Appendix 1 of this Agreement;
2. take all reasonable measures to prevent unauthorized access to the Impact Personal Data through the use of appropriate physical and logical (passwords) entry controls, securing areas for data processing, and implementing procedures for monitoring the use of data processing facilities;
3. build in system and audit trails;
4. account for all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of Impact Personal Data;
5. maintain the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
6. maintain the ability to restore the availability and access to Impact Personal Data in a timely manner in the event of a physical or technical incident;
7. implement a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Impact Personal Data;
8. monitor compliance on an ongoing basis; and
9. implement measures to identify vulnerabilities with regard to the processing of Impact Personal Data in systems used to provide Services to the Controller.