Handelsweg 6-1
3707 NH, Zeist
The Netherlands

T: +31 (0)30 697 32 88
Info@onetrail.com
www.onetrail.com

Data Processing Agreement

Onetrail as Processor

21 June 2022 Version 1.5

Chamber of Commerce: 23045776
VAT.: NL005588601B01

The undersigned

Onetrail B.V. a company incorporated under the laws of the Netherlands with its registered office in3707NH Zeist, Handelsweg 6 and registered in the Trade Register of the Chamber of Commerce under number 23045776 (hereinafter referred to as: "Processor"),

and

<Organization Name>
a company incorporated under the law of the <Country>. with its registered office in

<address, postal code, city>
and registered in the Trade Register of the Chamber of Commerce under number

.... (Hereinafter referred to as: "Controller"),

hereinafter collectively referred to as: "Parties" and each individually as a "Party".
declare to have agreed the following:

The Parties consider the following

(a) The Parties have concluded one or more specific contract(s) ("Service Agreement(s)") where Controller makes use of Onetrail B.V. for the performance of certain services ("the Services"). These Services may involve the processing of personal data in the sense of the General Data Protection Regulation (GDPR).

(b) For the processing of personal data on behalf of Controller, Onetrail B.V. functions as the Processor and Controller as the Controller in the sense of the GDPR, as the former will process personal data for the latter, without being subject to its authority and the Controller determines the purposes and the means of the processing of personal data.

(c) The Processor is qualified to perform these tasks.

(d) To enable the Parties to execute their relationship in a manner that is in accordancewith the law, the Parties have entered into this Data Processing Agreement ("DPA"),

as follows:

1. Definitions

Under this DPA, the following meanings are understood:

“Annex” appendix to the DPA, which forms an integral part of this Data Processing Agreement.

"Applicable Data Protection Act" the legislation that provides protection for the fundamental rightsand freedoms of individuals and in particular their right to privacy regarding the Processing of Personal Data, which legislation applies to the Controller and the Processor; the term Applicable Data Protection Act also includes the GDPR that entered into force 20 days after publication (4 May 2015). and became applicable as of 25 May 2018.

"Controller" the client of the Processor who, as a natural or legal person, alone or jointly with others, determines the purpose and means for the Processing of Personal Data.

"General Data Protection Regulation" or "GDPR" the Regulation {EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals regarding the processing of personal data and on the free movement of such data that entered into force 20 days after publication (4 May 2016) and became applicable as of May 25th, 2018.

"International Organization" an organization and its bodies governed by public international law orother bodies set up by or under an agreement between two or more countries.

"Member State" a country which belongs to the European Union.

"Personal Data" any information concerning an identified or identifiable natural person {DataSubject), which are processed by the Processor for the benefit of the Controller under this DPA.

"Data Subject" an identifiable person who can be identified directly or indirectly, in particular by means of an identifier such as a name, an identification number, location data, an on-line identifier orone or more elements that characterize the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

"Infringement in connection with Personal Data" a breach of security that inadvertently or unlawfully leads to the destruction, loss, modification, or unauthorized disclosure of or unauthorizedaccess to transmitted, stored or otherwise Processed data.

"Processing" an operation or a whole of operations relating to Personal Data or a body of Personal Data, whether or not performed via automated processes, such as collecting, recording, organizing,structuring, storing, updating, or modifying, retrieving, consulting, using, providing by means of forwarding, distributing or otherwise making available, aligning, or combining, blocking, erasing or destroying data.

"Processor" Processor who processes on behalf of the Data Controller.

"Service Agreement" the main agreement concluded between the Controller and the Processor andsetting out the conditions for the provision of the Services.

"Services" the Services provided by the Processor to the Controller and described under 'subject ofprocessing' in Annex 1 to this DPA.

"Special Categories of Data" data showing race or ethnic origin, political opinions, religious or philosophical beliefs or membership of a trade union; genetic data, biometric data processed for theunique identification of a natural person; data on health, or data related toa person's sexual behavior or sexual orientation.

"Sub-processor" a data processor who is called in by the Processor and who declares that he/she is willing to receive Personal Data from the Processor that are exclusively intended for Processing activities that must be performed for the Controller in accordance with his instructions, the terms and conditions of this DPA and the conditions of a written sub-processing agreement.

"Supervisory Authority" an independent public authority established by a Member State in accordance with Article 51 of the GDPR.

"Technical and Organizational Security Measures" the measures aimed at protecting Personal Data against unintentional destruction or accidental loss, modification, unauthorized disclosure, or access,where the Processing involves the transmission of data via a network, and against all other unlawful farms of Processing.

"Third Country" a country in respect of which the European Commission has not decided that that country, or an area or one or more specified sectors within that country, guarantees an adequate level of protection.

2. Rights and obligations of the Controller

If and to the extent the assignment under the applicable Services Agreement(s) entails the Processing of Personal Data of the Controller, this DPA is applicable thereto. The Controller remains the responsible data controller for the Processing of Personal Data in accordance with the instructions to the Processor under the Service Agreement, this DPA and any other instructions. The Controller has instructed the Processor and will continue to instruct the Processor for the duration of the commissioned data processing, to only process the Personal Data for the benefit of the Controller and in accordance with the Applicable Data Protection Act, the Service Agreement, this DPA and the instructions of the Controller. The Controller is entitled and obliged to instruct the Processor in connection with the Processing of the Personal Data, both in general and in individual cases. The instructions may also relate to the rectification, deletion and blocking of the Personal Data. The instructions are generally given in writing or by email, unless the urgency or other specific circumstances require a different (tor example verbal or electronic) form. Non-written or e-mailed instructions must be confirmed by the Controller in writing or by e-mail without delay. lnsofar as the execution of an instruction leads to costs for the Processor, the Processor will first inform the Controller of these costs. Only after the Controller has confirmed that the costs for the execution of an instruction are for his account, will the Processor carry out that instruction.

3. Obligations of the Processor

The Processor will:

(a) Process the Personal Data exclusively in accordance with the instructions of the Controller and on behalf of the Controller; these instructions are given in the Service Agreement, this DPA and otherwise in a documented form as mentioned in Article 2 above. This obligation to follow the instructions of the Controller also applies to the transfer of the Personal Data to a Third Country or an International Organization.

(b) inform the Controller immediately if the Processor cannot comply with instructions from the Controller for any reason.

(c) ensure that persons authorized by the Processor to Process the Personal Data for the Controller, commit to observe secrecy or that appropriate confidentiality is imposed on those persons and that the persons who have access to the Personal Data, will Process that Personal Data in accordance with the instructions of the Controller.

(d) implement the Technical and Organizational Security Measures that meet the requirements of the Applicable Data Protection Act as further specified in Annex 2 before Processing the Personal Data and ensure that he provides sufficient guarantees to the Controller with respect to those Technical and Organizational Security Measures.

(e) assist the Controller by means of appropriate Technical and Organizational Measures, to the extent feasible, for the fulfilment of the obligation of the Controller to respond to requests for exercising the rights of Data Subjects regarding information, access, rectification and deletion, limitation of processing, notification, data transferability, objection and automated decision-making; insofar as these achievable Technical and Organizational Measures require changes or adjustments to the Technical and Organizational Measures as listed in Annex 2, the Processor will inform the Controller of the costs of implementing such additional or altered Technical and Organizational Measures. As soon as the Controller has confirmed thatthese costs are for his account, the Processor will implement these additional or altered Technical and Organizational Measures to assist the Controller in responding to requests from Data Subjects.

(f) take appropriate measures to provide continuity and security of service. A certification or statement is available to support these measures. In case of a potential data breach Processor may transfer the Personal Data to a different location and/or environment, using a different Sub-Processor.

(g) make all information available to the Controller that is required to demonstrate compliance with the obligations set out in this DPA and in Art 28 GDPR, and make inspections possible, including inspections by the Controller or another inspector mandated by the Controller, and contribute to them. The Controller is aware that inspections in person and on location can significantly disrupt the business activities of the Processor and may cost a lot of time and money. The Controller may therefore only carry out an inspection in person and on locationif the Controller reimburses the Processor for the costs incurred by the Processor because of the disruption of the business activities.

(h) inform the Controller without undue delay:

i. of any legally binding request for the provision of the Personal Data by a law enforcement agency, unless this notification is otherwise prohibited, such as a criminal law prohibition to preserve the confidentiality of a law enforcement investigation.

ii. of complaints and requests received directly from the Data Subjects (such as complaints and requests for access, rectification, removal, limitation of processing, data transferability, objection to processing of data, automated decision-making) without goinginto that request, unless he is otherwise authorized to do so.

iii. if the Processor is required by EU legislation or the law of a Member State that applies to the Processor to process the Personal Data outside the scope of the assignmentof the Controller, before carrying out such processing outside that framework, unless suchEU legislation or legislation of that Member State forbids such information for important public interest reasons; that notification must state the legal requirement under that EU legislation or the legislation of the Member State.

iv. if, in the opinion of the Processor, an instruction conflicts with the Applicable DataProtection Act; when providing this notification, the Processor is not obliged to follow the instructions, unless and until the Controller has confirmed or modified them; and

v. as soon as the Processor becomes aware of a lnfringement in connection with Personal Data, at the Processor premises or on the systems used by the Processor to perform the Services under the applicable Service Agreement, at the latest within 24 hours after discovery. If the root cause is not yet discovered within said 24-hour time frame, the Processor will provide the Controller with the information available in order to enable the Controller to at least submit a preliminary breach notification to the Supervisory Authority.

vi. In the event of such a lnfringement in connection with Personal Data, the Processor will, at the written request of the Controller, assist with the obligation of the Controller pursuant to the Applicable Data Protection Act to inform the Data Subjects and the Supervisory Authorities respectively, and document the lnfringement in connection with Personal Data. Contact details regarding the report are recorded in the CRM/ERP package of the Processor. Contactsare specified in Annex 1;

(i) assist the Controller with a Data Protection Impact Assessment as required by Article 35 ofthe GDPR relating to the Services provided by the Processor to the Controller and the Personal Data processed by the Processor for the Controller.

(j) deal with all questions from the Controller regarding its Processing of the Personal Data to be processed (for example by enabling the Controller to respond in a timely manner to complaints or requests from the Data Subjects) and comply with the advice of the Supervisory Authority regarding the Processing of the transmitted data.

(k) insofar as the Processor is obliged and requested to rectify, delete and/or black any Personal Data processed based on this DPA, do so without delay. lf and insofar as Personal Data cann ot be deleted based on legal requirements relating to data retention, the Processor must, instead of deleting the relevant Personal Data, restrict the further Processing and/or the further use of Personal Data, or remove the associated identity from the Personal Data.

4. Obligations of the Controller

(a) The Controller guarantees the Processor that the Processing of Personal Data commissioned by or on behalf of the Controller is not unlawful and does not infringe the rights of Data Subjects, and that the Personal Data have been obtained in a manner that is compliant with the applicable statutory regulations.

5. Sub-processing

(b) The controller gives permission for the use of Sub-processor(s) that are engaged in by the Processor for the provision of the Services. The Controller gives his approval for the Sub- processor(s) as specified on the website of Processor under "Sub-Processors": https://onetrail.com/privacy-conditions/

(c) In the event that the Processor intends to enable new or more Sub-processors, the Processor shall ensure that the Sub-Processor page on the website is updated. Controller will be informed by Processor about changes in the Sub-Processor list on the website. lf the Controller has reasonable grounds to object to the use of new or more Sub-processors, the Controller must immediately notify this in writing within 14 days of receipt of the Sub- processor Notification. In the event that the Controller objects to a new or different Sub- processor, and that objection is not unreasonable, the Processor will make reasonable efforts to make changes to the Services available to the Controller, or to recommend a commercially reasonable change in the configuration of the Controller or the use by the Controller of the Services, for the prevention of Processing of Personal Data by the new or other Sub-processor against whom has been objected, without unreasonably burdening the Controller. If the Processor cannot make this change available within a reasonable period, which period shall not exceed sixty (60) days, the Controller may terminate the affected part of the Services Agreement, however only regarding those Services that cannot be provided by the Processor without the use of the new or other Sub-processor objected to by means of written notification to the Processor.

(d) The processor chooses the Sub-processor with the necessary care.

(e) lf such a Sub-processor is in a Third Country, at the written request of the Controller,the Processor will enter an EU model contract (Controller> Processor) for the Controller (in the name of the Controller), pursuant to Decision 2010/87/EU. In this case, theController instructs and authorizes the Processor to instruct the Sub-processors on behalf of the Controller, and to use all the rights of the Controller towards the Sub-processors based on the EU model contract.

(f) Without prejudice to the contents of clause 6 of the DPA, the Processor remains liable to the Controller for compliance with the obligations of the Sub-processor if the Sub-processor does not fulfil its obligations. However, the Processor is not liable for damage and claims arising from instructions from the Controller to Sub-processors.

6. Limitation of liability

(a) The Controller is fully responsible and is therefore liable for the intended purpose of the Processing, the content of the Personal Data entered by or on behalf of it or otherwise provided, its instructions, including the provision to third parties, the duration of the storage of the Personal Data, the ways of Processing and the means used for that purpose, except in so far as any act or omission is attributable to the Processor.

(b) All liability arising from or in connection with this DPA follows, and is exclusively governed by, the liability provisions set out in, or otherwise applicable to, the Service Agreement. Therefore, and in order to calculate liability limits and/or to determine the application of other limitations of liability, any liability arising under this DPA is deemed to arise under the relevant Services Agreement.

(c) If liability for corruption, loss and unlawful Processing of Personal Data is excluded or has not been stipulated under the Services Agreement, the Processor's liability vis-à-vis the Controller, contrary to the above, for corruption, loss and unlawful processing of the Personal Data pursuant to or in relation to this DPA, regardless of the basis of the claim, shall be limited to compensation of direct damages imputable to the Processor to the cumulative maximum amount included in the Services Agreement.

(d) The Controller is fully responsible and is therefore liable for the intended purpose of the processing, the content of the Personal Data entered or on behalf of it or otherwise provided, its instructions, including the provision to third parties, the retention period of the Personal Data, the ways of Processing and the means used for that purpose, except in so far as any act or omission is attributable to the Processor.

(e) The Processor is under no circumstance liable for a fine imposed on the Controller by a data protection authority, in the event the data protection authority has taken the degree to which blame can be attributed into consideration and has imposed the fine() accordingly on the Party/Parties concerned or in the event the Processor has not been involved in the enforcement proceedings and/or has not been provided the opportunity to defend itself, including but not limited to have been provided the opportunity to state its views as referred to in Article 4:8 of the Dutch General Administrative Law Act.

7. Duration and termination

(a) The duration of this DPA is equal to that of the relevant Services Agreement. Unless otherwise stipulated in this agreement, rights, and obligations in the area of termination arethe same as the rights and obligations included in the relevant Services Agreement. This Data Processing Agreement will end by operation of law if all Service Agreements between Parties have terminated or expired.

(b) The Processor must, at the discretion of the Controller, a) delete all Personal Data after the end of the provision of the Services or b) return it to the Controller and delete all existing copies unless the Processor is required by EU or Member State law to retain that Personal Data. The Processor shall be entitled to charge the Controller for any costs involved. The Controller shall be obliged to inform the Processor of its choice for sub a) or b) in due time and in writing before the end of the applicable Service Agreement, unless this cannot be reasonably expected from the Controller, in which event the reasoned request is to be sent to the Processor ultimately within two calendar weeks following the end of applicable Services Agreement unless Parties agree upon another period within the context of an exit strategy.

8. Other

(a) In the event of any conflict between the provisions in this DPA and any other agreements between the Parties, the provisions in this DPA regarding the data protection obligations of the Parties shall prevail. In case of doubt as to whether clauses in these other agreements relate to the data protection obligations of the Parties, this DPA shall prevail.

(b) invalidity or unenforceability of any provision in this DPA does not affect the validity or enforceability of the other provisions of this DPA. The invalid or unenforceable provision is (i) amended to guarantee its validity or enforceability while at the same time preserving the Parties' intentions as much as possible or - if this is not possible - (ii) interpreted as if the invalid or unenforceable part had never been included therein. The foregoing also applies if this DPA contains an omission.

(c) This DPA is governed by the same legislation as the Service Agreement, except insofar as mandatory Applicable Data Protection Law applies.

On behalf of the Controller:

(Full) Name:

Function:

Date:

Signature:

On behalf of Processor:

(Full) Name: T. Berkers

Function: Managing Director

Date: June 21st, 2022

Signature:

Annex 1 - Categories of Data Subjects

The transmitted Personal Data concern the following categories of Data subjects:

Customers of the Controller
Business relations and contact persons of the Controller
Employees of the Controller
Suppliers of the Controller

Subject of the processing

Use of Service(s) in accordance with the applicable Service Agreement(s).

Nature and purpose of the processing

The Processor collects. processes and uses the Personal Data of the Data Subjects for the benefit of the Controller. to execute the Service agreement(s).

Location(s) of processing

Processor processes the Personal Data in the NorthC Datacenter located in Almere the Netherlands.

Type of personal data

The Personal Data collected. processed and used by the Processor on behalf of the Controller concern the following categories of personal data:

- Name
- Function
- Gender
- Language
- Address
- E-Mail address
- Telephone number

Contact details

lf the Controller wants to process personal data of the type "Special Categories of Data". the Controller must always contact the Processor first, in writing or by mail.

Contact information in case of data leaks

Controller
Processor: security@onetrail.com

Annex 2 - Security measures Sheet

Description of the Technical and 0rganizational Security Measures implemented by the Processor in accordance with the Applicable Data Protection Act:
This Annex describes the minimum Technical and 0rganizational Security Measures and procedures that the Processor must maintain, in order to protect the security of personal data created, collected, received or otherwise obtained.

General: Technical and organizational measures can be regarded as the state of the art at the time of the conclusion of the Services Agreement. The processor will evaluate technical and organizational measures over time, considering casts for transit, nature, scope, context and processing objectives, and the risk of differencesin the likelihood and severity of the rights and freedoms of natural persons.

Detailed technical measures:	**Status**	**Optionality**	**Available certification**
Pseudonymization of data	Present: With special personaldata on test systems	0ptional	
Encryption of data	Present: With special personaldata (passwords). Backups are encrypted	Mandatory	
Ability to guarantee continued confidentiality, integrity, availability and resilience of processing systems and services	Present		ISO 27001
Ability to restore the availability of and access to the Personal Data in the event of aphysical or technical incident, in a timely manner.	Present		ISO 27001
Process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the safety of the processing.	Present		ISO 27001