

DATA PROCESSING ADDENDUM (TYPEFORM AS VENDOR)

This Data Processing Addendum ("**Addendum**") forms part of the main agreement ("**Principal Agreement**") entered into between (i) stichting veul ("**Company**") or "**Client**") acting on its own behalf and as agent for each Company Affiliate; and (ii) Typeform, S.L. ("**TYPEFORM**") acting on its own behalf and as agent for each TYPEFORM Affiliate.

By signing the Agreement, TYPEFORM enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of any authorized Subprocessor.

In the course of providing the Services to Client by TYPEFORM pursuant to the Agreement, TYPEFORM may process Personal Data on behalf of Client and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. OBJECT

- 1.1. The present Addendum regulates the terms and conditions that will apply to the treatment of Personal Data that TYPEFORM may have access by virtue of the Services.
- 1.2. For the purposes of the present Addendum, terms shall have the meanings set out in Annex 1.2.

2. PROCESSING OBJECTIVES

- 2.1.** TYPEFORM undertakes to process personal data on behalf of the Company in accordance with the conditions laid down in this Data Processing Agreement. The processing will be executed exclusively within the framework of the Agreement, and for all such purposes as may be agreed to subsequently.
- 2.2.** TYPEFORM shall refrain from making use of the personal data for any purpose other than as specified by the Company. The Company will inform TYPEFORM of any such purposes which are not contemplated in this Data Processing Agreement.
- 2.3.** All personal data processed on behalf of the Company shall remain the property of the Company and/or the relevant Data subjects.
- 2.4.** TYPEFORM shall take no unilateral decisions regarding the processing of the personal data for other purposes, including decisions regarding the provision thereof to third parties and the storage duration of the data.
- 2.5.** Annex 2.5 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Company Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Company may make reasonable amendments to Annex 2.5 by written notice to TYPEFORM from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Annex 2.5 confers any right or imposes any obligation on any party to this Addendum.

3. TYPEFORM'S OBLIGATIONS

- 3.1.** TYPEFORM shall warrant compliance with the applicable laws and regulations, including laws and regulations governing the protection of personal data.
- 3.2.** TYPEFORM shall furnish the Company promptly on request with details regarding the measures it has adopted to comply with its obligations under this Addendum.
- 3.3.** TYPEFORM's obligations arising under the terms of this Addendum apply also to whomsoever processes Company Personal Data under the TYPEFORM's instructions.

4. TYPEFORM AND TYPEFORM AFFILIATE PERSONNEL

- 4.1.** TYPEFORM and each TYPEFORM Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant Company Personal Data, as strictly necessary

for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. SECURITY

- 5.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, TYPEFORM and each TYPEFORM Affiliate shall implement appropriate technical and organizational measures to protect the Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the Data (a "**Security Incident**"). At a minimum, such measures shall include the security measures identified Appendix 2 to Annex 5.1
- 5.2. In assessing the appropriate level of security, TYPEFORM and each TYPEFORM Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.
- 5.3. Security incidents: Upon becoming aware of a Security Incident, TYPEFORM shall inform the Company without undue delay (and, in any event, within 24 hours) and shall provide all such timely information and cooperation as The Company may require in order for the Company to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. TYPEFORM shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep the Company informed of all developments in connection with the Security Incident. TYPEFORM shall not notify any third parties of a Security Incident affecting the Data unless and to the extent that: (a) the Company has agreed to such notification (such agreement not to be unreasonably withheld, conditioned or delayed), and/or (b) notification is required to be made by TYPEFORM under Applicable Data Protection Law.

6. SUBPROCESSING

- 6.1. Each Company Group Member authorizes TYPEFORM and each TYPEFORM Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Principal Agreement.
- 6.2. TYPEFORM and each TYPEFORM Affiliate may continue to use those Subprocessors already engaged by TYPEFORM or any TYPEFORM Affiliate as at the date of this Addendum, subject to TYPEFORM and each TYPEFORM Affiliate in each case as soon as practicable meeting the obligations set out in section 6.4.
- 6.3. TYPEFORM shall give Company prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 30 days of receipt of that notice,

Company notifies TYPEFORM in writing of any objections (on reasonable grounds) to the proposed appointment, neither TYPEFORM nor any TYPEFORM Affiliate shall appoint (or disclose any Company Personal Data to) that proposed Subprocessor until necessarily and reasonable steps have been taken to address the objections raised by any Company Group Member and Company has been provided with a reasonable written explanation of the steps taken.

6.4. With respect to each Subprocessor, TYPEFORM or the relevant TYPEFORM Affiliate shall:

6.4.1. Before the Subprocessor first Processes Company Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement.

6.4.2. Ensure that the arrangement between on the one hand (a) TYPEFORM, or (b) the relevant TYPEFORM Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand, the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR.

6.4.3. If that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) TYPEFORM, or (b) the relevant TYPEFORM Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Company Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Company Group Member(s) (and Company shall procure that each Company Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution).

6.4.4. Provide to Company for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Company may request from time to time.

6.5. TYPEFORM and each TYPEFORM Affiliate shall ensure that each Subprocessor performs the obligations under this Addendum, as they apply to Processing of Company Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of TYPEFORM.

7. DATA SUBJECT RIGHTS

- 7.1.** Taking into account the nature of the Processing, TYPEFORM and each TYPEFORM Affiliate shall assist each Company Group Member by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.
- 7.2.** TYPEFORM shall:
 - 7.2.1.** Promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data.
 - 7.2.2.** Ensure that the Contracted Processor does not respond to that request except on the documented instructions of Company or the relevant Company Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case TYPEFORM shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

8. PERSONAL DATA BREACH

- 8.1.** TYPEFORM shall notify Company without undue delay upon TYPEFORM or any Subprocessor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
- 8.2.** TYPEFORM shall co-operate with Company and each Company Group Member and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

- 9.1.** TYPEFORM and each TYPEFORM Affiliate shall provide reasonable assistance to each Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. DELETION OR RETURN OF COMPANY PERSONAL DATA

- 10.1.** Upon termination or expiry of the Agreement, TYPEFORM shall (at Company's election) destroy or return to Company all Company Personal Data (including all copies of the Data) in its possession or control (including any data subcontracted to a third party for processing). This requirement shall not apply to the extent that TYPEFORM is required by any applicable law to retain some or all of the Data, in which event TYPEFORM shall isolate and protect the Data from any further processing except to the extent required by such law.
- 10.2.** Upon request by Company, TYPEFORM shall provide a written certification that it has complied with the requirements of this Section signed by an officer of TYPEFORM.

11. AUDIT RIGHTS

- 11.1.** Either following a security incident suffered by TYPEFORM, or upon the instruction of a data protection authority, TYPEFORM shall permit the Company that is not a competitor of TYPEFORM (or its appointed third party auditors) to audit TYPEFORM's compliance with this Addendum, and shall make available to the Company all information, systems and staff necessary for the Company (or its third party auditors) to conduct such audit. TYPEFORM acknowledges that the Company (or its third-party auditors) may enter its premises for the purposes of conducting this audit, provided that the Company gives it reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to TYPEFORM's operations. Such audit will be subject to any confidentiality terms agreed between the parties.

12. RESTRICTED TRANSFERS

- 12.1.** Each Company Group Member (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Company Group Member to that Contracted Processor.
- 12.2.** The Standard Contractual Clauses shall come into effect on the later of:
 - 12.2.1.** The data exporter becoming a party to them.
 - 12.2.2.** The data importer becoming a party to them.
 - 12.2.3.** Commencement of the relevant Restricted Transfer.

12.3. Section 12.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12.4. TYPEFORM warrants and represents that, before the commencement of any Restricted Transfer to a Subprocessor which is not a TYPEFORM Affiliate, TYPEFORM's or the relevant TYPEFORM Affiliate's entry into the Standard Contractual Clauses, and agreement to variations to those Standard Contractual Clauses, as agent for and on behalf of that Subprocessor will have been duly and effectively authorized (or subsequently ratified) by that Subprocessor.

13. GENERAL TERMS

13.1. Governing law and jurisdiction

13.1.1. The Addendum and the implementation thereof will be governed by Spanish law.

13.1.2. Any dispute which may arise in connection with and/or arising from this Addendum shall be governed by the courts of the City of Barcelona (Spain).

13.2. Order of precedence

13.2.1. Nothing in this Addendum reduces TYPEFORM's or any TYPEFORM Affiliate's obligations under the Principal Agreement in relation to the protection of Personal Data or permits TYPEFORM or any TYPEFORM Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.


13.2.2. Subject to section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.


13.3. Severance

13.3.1. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while

preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

[Client]
Signature 
Name Stichting Veul Diech Good, Anton Vegers voorzitter
Title voorzitter
Date Signed 29-5-2018 16:43:08 PDT

TYPEFORM, S.L.
Signature 
Name Robert Muñoz
Title CEO
Date Signed 29-5-2018 16:43:08 PDT

ANNEX 1.2: DEFINITIONS

In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1. "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Company Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;
2. "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;
3. "**Company Group Member**" means Company or any Company Affiliate;
4. "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Company Group Member pursuant to or in connection with the Principal Agreement;
5. "**Contracted Processor**" means TYPEFORM or a Subprocessor;
6. "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;
7. "**EEA**" means the European Economic Area;
8. "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;
9. "**GDPR**" means EU General Data Protection Regulation 2016/679;
10. "**Restricted Transfer**" means:
 - (i) a transfer of Company Personal Data from any Company Group Member to a Contracted Processor; or
 - (ii) an onward transfer of Company Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor

In each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address

the data transfer restrictions of Data Protection Laws) in the absence of (i) the Standard Contractual Clauses, or (ii) a self-certification to the Privacy Shield (to be maintained for so long as TYPEFORM processes the Company Personal Data), assuming that the scope of such self-certification covers all Company Personal Data that TYPEFORM processes under the Agreement and this Addendum, and TYPEFORM agrees to comply with the Privacy Shield Principles when processing any such Company Personal Data.

11. "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of TYPEFORM for Company Group Members pursuant to the Principal Agreement;
 12. "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 5.1, amended as indicated (in square brackets and italics) in that Annex;
 13. "**Subprocessor**" means any person (including any third party and any TYPEFORM Affiliate, but excluding an employee of TYPEFORM or any of its sub-contractors) appointed by or on behalf of TYPEFORM or any TYPEFORM Affiliate to Process Personal Data on behalf of any Company Group Member in connection with the Principal Agreement; and
 14. "**TYPEFORM Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with TYPEFORM, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.
- 1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.
- 1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

ANNEX 2.5: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 2.5 includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Company Personal Data

The subject matter and duration of the Processing of the Company Personal Data are set out in the Principal Agreement and this Addendum.

The nature and purpose of the Processing of Company Personal Data

The personal data transferred will be subject to the following basic processing activities:

Only used to provide relevant Typeform service as set forth in our T&Cs and Privacy policy

The types of Company Personal Data to be Processed

Email address, name, billing information and enriched data from 3rd parties (where applicable) and product usage data

The categories of Data Subject to whom the Company Personal Data relates

Typeform Account holders

The obligations and rights of Company and Company Affiliates

The obligations and rights of Company and Company Affiliates are set out in the Principal Agreement and this Addendum.

ANNEX 5.1: STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection [*This opening recital is deleted if these Clauses are not governed by the law of a member state of the EEA.*]

[*The gaps below are populated with details of the relevant Company Group Member:*]

Name of the **data exporting organisation**: Stichting veul Diech Good
Address: Geulhout 12, 6241 DH Bunde Nederland
Tel.: 06-29460091; e-mail: info@stichtingveuldiechgood.nl
Other information needed to identify the organisation

.....
(the data **exporter**)

And

[*The gaps below are populated with details of the relevant Contracted Processor:*]

Name of the **data importing organisation**: Typeform S.L
Address: Bac de Roda 163, 08018, Barcelona, Spain
Tel.: _____; e-mail: gdpr@typeform.com
Other information needed to identify the organisation:

.....
(the data **importer**)
each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1
Definitions

For the purposes of the Clauses:

- (a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; [*If these*

Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words "except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data" are added.]

- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC; [*If these Clauses are not governed by the law of a Member State, the words "and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC" are deleted.*]
- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to

exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;

- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC; *[If these Clauses are not governed by the law of a Member State, the words "within the meaning of Directive 95/46/EC" are deleted.]*
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:

- (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that

the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12
Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): Stichting Veul Diech Good, Anton Vegers voorzitter

Position: Voorzitter

Address: Geulhout 12, 6241 DH Bunde Nederland

Other information necessary in order for the contract to be binding (if any):

Signature.....

DocuSigned by:

Stichting Veul Diech Good, U

8F33082E8B014B6...

On behalf of the data importer:

[Populated with details of, and deemed signed on behalf of, the data importer:]

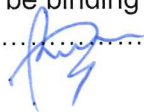
Name (written out in full): Robert Munoz

Position: CEO

Address: Bac de Roda 163, 08018, Barcelona, Spain

Other information necessary in order for the contract to be binding (if any):

Signature.....



APPENDIX 1 TO ANNEX 5.1 (STANDARD CONTRACTUAL CLAUSES)

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter Stichting Veul Diech Good

The data exporter is: -----

Data importer

TYPEFORM is a Barcelona based online Software as a Service platform that specializes in online form building and online surveys. Its main software helps to create dynamic forms based on user needs.

Data subjects

The personal data transferred concern the following categories of data subjects:

Typeform Account holders

Categories of data

The personal data transferred concern the following categories of data:

Email address, name, billing information and enriched data from 3rd parties (where applicable) and product usage data

Special categories of data (if appropriate)

NA

Processing operations

The personal data transferred will be subject to the following basic processing activities:

Only used to provide relevant Typeform service as set forth in our T&Cs and Privacy policy

DATA EXPORTER

----- Stichting Veul Diech Good

Name: Stichting Veul Diech Good, Anton Vegers voorzitter

Authorized Signature *Stichting Veul Diech Good, Anton Vegers voorzitter*

8F33082E8B01496...

DATA IMPORTER

TYPEFORM S.L

Name: Robert Munoz

Authorized Signature

APPENDIX 2 TO ANNEX 5.1 (STANDARD CONTRACTUAL CLAUSES)

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures to be implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. Information Security Program (ISP)

Supplier will maintain an ISP designed to (a) help Typeform secure Personal Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the Supplier Network (defined below), and (c) minimize security risks, including through risk assessment and regular testing. Supplier will appoint an employee to be accountable for the ISP.

The ISP will include the following measures:

1.1. Network Security

The Supplier Network will be accessible to employees, contractors and any other person as required to provide the data processing services. Supplier will maintain access controls and policies to manage access to the Supplier Network from each network connection and user, including the use of authentication controls, firewalls or Intrusion Detection systems. Supplier will maintain security incident response plans to handle potential security incidents.

1.2. Physical Security

Physical components of the Supplier Network are housed in facilities ("Facilities") controlled by an ISO 27001 certified company (i.e. Amazon Web Services or Rackspace) or in Facilities which meet or exceed all of the following physical security requirements:

- (i) **Physical Access Controls.** Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.
- (ii) **Limited Employee and Contractor Access.** Supplier provides access to the Facilities to those employees and contractors who have a

legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of Supplier or its affiliates.

- (iii) **Physical Security Protections.** All access points (except for main entry doors) are maintained in a locked state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. Supplier also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

1.3. Personal Data Security. Controls for the Protection of Personal Data.

Supplier will maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of personal data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. Supplier regularly monitors compliance with these measures. Supplier will not materially decrease the overall security of the data processing services during a subscription term

1.4. Business Continuity and Disaster Recovery

Supplier will maintain a Business Continuity and Disaster Recovery plan based on risk. Recovery plan are tested at least annually to guarantee that full recovery is possible to meet expected SLA's.

1.5. Employee security

Supplier will have signed confidentiality agreements with the employees and contractors. For positions with access to personal information, background checks are also performed. Also, all employees and contractors will have a common way to report incidents approved by the organization and they will undergo at least an annual security awareness training.

2. Ongoing Evaluation

Supplier must reassess and update their security policies on a periodic basis. Changes must be documented and employ change controls.

Annex 6.1

Authorized Sub-processors

Please find the list of our sub-processors in the link below. The list will be updated as and when the sub-processors are changed.

<https://www.typeform.com/help/what-other-companies-do-we-share-data-with/>

Controller acknowledges and agrees that the entities in the above list shall be deemed authorized sub-processors that may process personal data pursuant to this addendum.