Confidential

Data Processing Agreement

Data Processing Agreement between

(Controller Name) Jikke Patist Fotografie

and **WeTransfer B.V.**

Parties:

1. (Name Company client) Jikke Patist Fotografie
having its registered and business office in
(Address) Nolenslaan 31 1, 3515 VB Utrecht
represented by (Name) Jikke Patist
hereinafter 'Controller'; and

2. WeTransfer B.V. having its registered and business office in Oostelijke Handelskade 751, represented by Nienke Koorn, hereinafter 'Processor';

Whereas:

A. Under the General Data Protection Regulation, any information relating to an identified or identifiable natural person that is part of an upload done from within the European Union by the Controller using the Processor, is defined as 'personal data', hereinafter: 'Personal Data'.

B. Controller has instructed Processor to provide services to Controller, whereby Processor processes Personal Data on behalf of and on account of Controller, and Controller determines the scope, means and validity of the processing;

C. Controller and Processor have confirmed their agreements regarding the processing of Personal Data by Processor as instructed Controller into this agreement hereinafter: 'Data Processing Agreement' or 'Agreement'.

Therefore, The Parties Agree As Follows:

1. Subject of this Agreement

1.1 This Data Processing Agreement applies to the services and activities carried out by Processor on behalf of Controller under the principle agreement Terms of Service, including the Privacy and Cookie Statement, hereinafter: 'Assignment'.

1.2 This Data Processing Agreement replaces all prior understandings between the Parties about the processing of Personal Data. Where the provisions of this Agreement contradicts or amends earlier agreements on the processing of Personal Data, the provisions of this Agreement prevail unless otherwise expressly provided in this Agreement.

1.3 Following this Agreement, Processor processes Personal Data on behalf of Controller and under Controller's responsibility.

1.4 Processor processes Personal Data exclusively for the purposes following execution of the Assignment.

1.5 Processor will process Personal Data only in accordance with the instructions of Controller. Processor has no independent control of Personal Data that it processes. Processor may not process Personal Data for its own benefit, the benefit of third parties or other purposes, except with Controller's prior written consent or where required by law.

1.6 If Processor is required by law to disclose or otherwise process personal data that is not in accordance with the instructions of the controller, the Processor will inform the Controller of these requirements prior to processing the Personal Data, unless that law prohibits such information on important grounds of public interest.

1.7 Controller is responsible for assessing whether the data processing is legitimate and for securing the rights of the data subjects.

1.8 Verbal instructions issued by Controller to Processor must be confirmed in writing, without delay.

2. Confidentiality

2.1 Processor shall keep Personal Data confidential and shall not disclose Personal Data in any way to the employees and/or third parties, except where, (i) it is necessary that employees and/or third parties need to have knowledge of Personal Data for the purpose of execution of the Assignment, or (ii) it is required by law.

2.2 Processor shall provide the employees and/or third parties access to Personal Data only to the extent necessary to perform the processing necessary for the execution of the Assignment. Processor ensures that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3. Sub-processors

3.1 Controller gives general authorisation to Processor for the addition or replacement of data processors under the conditions set out in this Agreement. Controller will be offered the possibility to object to changes concerning the addition or replacement of data processors, but the objection may not be disproportionate.

3.2 Processor enters into a written data processing agreement with all permitted sub-processors. Processor shall ensure that sub-processors are contractually bound to the same or higher obligations with respect to the processing as those which Processor is bound to under this Agreement.

4. Security and data breaches

4.1 Processor agrees to implement at least the technical and organisational security measures detailed in **Appendix A**, including procedures directed at reasonably detecting and acting on security incidents and data breaches, for the purpose of ensuring an appropriate level of protection for the processing of Personal Data within the scope of the Assignment.

4.2 Upon receiving knowledge of a (potential) security incident (e.g. a security breach) or (potential) data breach of Controller's Personal Data, Processor will notify Controller within 72 hours, if Controller is affected by this incident.

4.3 The notification as mentioned in article 4.2 will contain, for so far available, the following information:

1. The day and time that Processor knowledge received of the security incident;
2. The nature of the security incident;
3. The moment, or the most likely moment or period, the security incident has occurred and how long it lasted;
4. The range of Personal Data of Controller (possibly) involved in the security incident;
5. The possible consequences/risks of the security incident for the privacy of the data subjects, i.e. those involved;
6. The contact points where more information about the security incident can be obtained;
7. The recommended measures to reduce the negative consequences of the security incident;
8. The measures that Processor has taken or proposes to take to remedy the security incident.
9. All other information that is relevant to assess the security incident.

4.4 With respect to each security incident referred to in article 4.2 Processor shall provide all assistance to Controller that can reasonably be expected of Processor, including the provision of adequate information and support regarding the provision of information referred to in article 4.3. and article 4.4, inquiries from authorities, limiting the impact of a security incident on the privacy of the data subject (s) and/or limiting Controller's damage as a result of the security incident.

4.5 Processor will evaluate its security measures with regard of Personal Data processing following the Assignment regularly, based on the ISO/IEC 27000 series or similar standards.

5. Transfer of Personal Data

5.1 Controller acknowledges that Processor or any subcontractor engaged by Processor may transfer Personal Data to countries outside the European Union or an international organisation governed by public international law, including making Personal Data available or accessible, if this processing is as secure as processing within the European Union would be.

5.2 In respect of such transfers and where no Alternative Level of Protection applies (such as the EU-US Privacy Shield), Processor shall ensure that in addition to the requirements described in this agreement, appropriate measures are taken to ensure a level of security adequate under the General Data Protection Regulation.

6. Right to audit

6.1 Processors shall make the processing systems, facilities and supporting documentation relevant to the processing of Personal Data available for an audit by a qualified independent assessor selected by Processor. Processor will provide reasonable and necessary cooperation to such audits and will ensure that its subcontractors do likewise.

6.2 An audit may be performed during Processor's normal working days and normal working hours, no more than once per year or if requested by a relevant authority, subject to notice given in advance with a reasonable notice period. The audit may take place at Processor's place of business by inspecting the stored Controller Personal Data in a storage facility or data centre and the Processing activities taking place at the premises of Processor in accordance with Processor's security and access policies.

6.3 Controller shall bear the costs of any audit that is requested additionally to the yearly audit described in 6.1.

7. Inspection or audits by public authorities

7.1 Processor shall submit its relevant processing systems, facilities and supporting documentation to an inspection or audit relating to the Processing by a competent public authority if this is necessary to comply with a legal obligation. In the event of any inspection or audit, each Party shall provide all reasonable assistance to the other Party in responding to that inspection or audit. If a competent public authority deems the Processing in relation to the Agreement unlawful, the Parties shall take immediate action to ensure future compliance with the applicable data protection laws.

8. Cooperation enquiries & data subject rights

8.1 Processor will provide its prompt and full cooperation, ultimately within 15 working days, with enquiries of Controller related to the Processing under the Agreement, including but not limited to any complaints, requests or enquiries received from data subjects. Processor shall not respond to data subjects directly except where specifically instructed by Controller.

8.2 Processor shall take reasonable technical and organisational measures to assist Controller in the fulfilment of the obligation to respond to requests for exercising the data subject rights as described in Chapter III of the General Data Protection Regulation insofar as this is possible.

9. Government agencies requests

9.1 Processor will only act on a request from a government agency to provide (access to) Personal Data if required by law and the request meets legal requirements, including the principles of proportionality and subsidiarity.

9.2 Processor informs Controller of a government agency request to process Personal Data, unless the government agency request expressly prohibits such notification.

10. Costs and Liability

10.1 The execution costs of this Agreement are included in the prices and fees agreed for the Assignment.

11. Indemnity

11.1 Controller shall indemnify and hold harmless Processor, its officers, directors, employees, contractors, and agents from and against all claims, liabilities, administrative fines, suits, judgments, actions, investigations, settlements, penalties, fines, damages and losses, demands, costs, expenses, and fees including reasonable attorneys' fees and expenses, arising out of or in connection with any claims, demands, investigations, proceedings, or actions brought by Data Subjects, legal persons (e.g., corporations and organizations), or supervisory authorities under the Data Protection Laws that apply to the Processor or any Sub-processor engaged by Processor in respect of the Personal Data Processed under this DPA and under the General Data Protection Regulation.

12. Return and destruction of Personal Data

12.1 Upon termination of the Agreement, Processor shall, at the option of Controller, securely delete and/or destroy Personal Data, except to the extent the Agreement or applicable laws provide otherwise. In that case, Processor shall no longer process the Personal Data, except to the extent required by the Agreement or applicable laws. Controller may require Processor to promptly and in any case within two weeks, confirm and warrant that Processor has deleted and/or destroyed all copies of the Personal Data.

12.2 Upon termination of the Agreement, Processor shall, at the option of Controller, return the Personal Data including any copies thereof to Controller and/or shall securely destroy such Personal Data, except to the extent the Agreement or applicable laws provide otherwise. In that case, Processor shall no longer process the Personal Data, except to the extent required by the Agreement or applicable laws. Controller may require Processor to promptly and in any case within two weeks, confirm and warrant that Processor has returned, deleted and/or destroyed all copies of the Personal Data.

13. Term and termination

13.1 This Agreement enters into force as soon as Processor commences Personal Data processing on behalf of Controller following execution of the Agreement. In case of an existing Assignment between Processor and Controller, this Agreement commences at the latest on May 25 2018.

13.2 This Agreement is effective for as long as the Assignment continues. Upon termination of the Assignment, this Agreement ends by operation of law.

13.3 Processor may terminate the Agreement prematurely, unless Controller indicates that processing of Personal Data as referred to under article 1.1 and 1.4 is longer necessary for the execution of the Assignment.

13.4 Any obligations under this Agreement that by their nature are intended to survive after termination of the Agreement will continue to apply after termination.

14. Changes and Renegotiations

14.1 Deviations from and additions to this Agreement are only valid if agreed explicitly and in writing.

14.2 Processor hereby agrees in advance to changes in the Agreement as a result of changes to the legal framework for protection of personal data that are strictly necessary for compliance with the relevant laws and regulations or the interpretation thereof or the policies of the authorities.

14.3 The Agreement will only be valid while the Controller follows and adheres to the accompanying Assignment as mentioned in clause 1.1. If the Controller fails to comply with any version of the accompanying assignment, no claim as stated in clause 11 can be made.

15. Miscellaneous

15.1 This Agreement is governed by Dutch law.

15.2 Disputes arising from this Agreement are submitted by exclusion to the agency competent to hear and decide on disputes arising from the Assignment. Failing such agency, the competent Court of Amsterdam (Netherlands) will have exclusive jurisdiction.

15.3 Any standard terms of business and other standard or special terms and conditions of Controller do not apply to this Agreement and are explicitly dismissed by Processor.

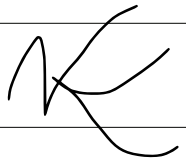
15.4 Processor does not have the right to transfer its rights and obligations under this Agreement to third parties without Controller's prior written consent.

Agreed And Signed:

Processor

Nienke Koorn
Name

Privacy Officer
Job title

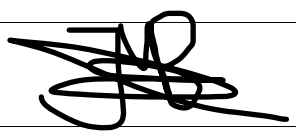


Date

Controller

Jikke Patist Fotografie
Name

Photographer
Job title



17-07-2020
Date

Appendix A

Technical and organisational security measures

1. **Data Access Controls:**
   Processor ensures that Personal Data is accessible and manageable only by properly authorised staff who need access to perform their tasks, direct database query access is restricted and activity by those who have access of logged to ensure the safety of the Personal Data; and, that Personal Data can only be read, copied, modified or removed by a select group of properly authorised staff in the course of Processing.

2. **Transmission Controls:**
   Processor ensures that Service Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport from the Controller to Processor. Transfers are encrypted when they are uploaded, downloaded and while they are hosted on the server of the Processor, and only sent over a secured (https) connection while they are transported from the Controller to the Processor and back.
   Transfers done from within the EU are stored only on EU servers owned by AWS, located in Dublin and fully GDPR compliant.

3. **Input Controls:**
   Processor shall monitor whether and by whom Data has been entered into Data processing systems, modified or removed. Processor shall take reasonable measures to ensure that (i) the Personal Data source is under control of Controller and accessible to Controller, and (ii) Personal Data integrated into the service is managed by secured transmission from Controller.

4. **Subprocessor Security:**
   Before on boarding Sub-processors, Processor will assess the security and privacy practices of Sub-processors to ensure they provide a level of security and privacy appropriate to their level of access to Personal Data and the scope of the services they provide. Sub-processors need to process Personal Data within the EU, or be part of the Privacy Shield certification.

5. **Personnel Security:**
   Processor's staff is required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, ethics, and appropriate usage of Personal Data. Staff is required to execute a confidentiality agreement and are provided with privacy and security training multiple times a year.

6. **Logical Separation:**
   Data from different Processor's subscriber environments is logically segregated on Processor's systems to ensure that Personal Data that is collected for different purposes may be Processed separately.

7. **Erasure of transfers:**
   When a transfer expires, the content of that transfer, including any personal data that was part of that content, will be scrubbed entirely from the server. That means there is no way to retrieve the content of a transfer after its expiration date.