WeTransfer Data Processing Agreement

Last update: March 18, 2025

This Data Processing Agreement ("**DPA**" or "**Agreement**") is entered into by and between WeTransfer B.V., with registered office at Keizersgracht 281, 1016 ED Amsterdam, the Netherlands ("**Provider**") and WeTransfer customer ("**Customer**"). Each of Customer and Provider may be referred to herein individually as the "**Party**" and collectively as the "**Parties**".

Whereas:

A. Customer has entered into Provider's Terms of Service or any other agreement (the "**Contract**") for the receipt of certain services from Provider as described in the Contract (the "**Service**").

B. In order to provide the Service, Provider will process personal data acting as the Data Processor on behalf and on account of Customer, which determines the scope and means of the processing, acting as the Data Controller.

C. The Parties enter into this DPA in order to ensure that they comply with Applicable Privacy Laws (as defined below) and establish safeguards and procedures for the lawful processing of personal data.

Therefore, the Parties agree as follows:

1. Definitions. When used in this Agreement, the following terms have the following meaning.

1.1 "**Applicable Privacy Laws**" means all applicable data protection laws and regulations, including but not limited to the EU General Data Protection Regulation 2016/679 ("**GDPR**").

1.2 "**Content**" means any file(s) the Customer uploads, creates, organizes, or otherwise uses in the Provider's products.

1.3 "**Data Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. For the purposes of this Agreement, Customer acts in its role as Data Controller.

1.4 "**Data Processor**" means the entity that Processes Personal Data on behalf of the Data Controller. For the purposes of this Agreement, Provider acts in its role as Data Processor.

1.5 **"Data Subject"** means an identified or identifiable natural person to which the Personal Data pertains.

1.6 "**Illegal content**" means Content that: (1) features CSAM (child sexual abuse material); (2) is obscene, defamatory, libelous, slanderous, profane, indecent, discriminating, threatening, abusive, harmful, lewd, vulgar, or unlawful; (3) promotes racism, violence or hatred; (4) is factually inaccurate, false, misleading, misrepresenting or deceptive; (5) you don't hold the rights to; (6) infringes, violates or misappropriates intellectual property rights, privacy rights, including data protection rights, and/or any other kind of rights; (7) infringes on or violates any applicable law or regulation; and/or (8) constitutes 'hate speech', whether directed at an individual or a group, and whether based upon the race, sex, creed, national origin, religious affiliation, sexual orientation,

language or another characteristic of such individual or group.

1.7 **"Instructions"** means this Agreement and any further written agreement or documentation by way of which the Data Controller instructs the Data Processor to perform specific Processing of Personal Data.

1.8 **"Personal Data"** means any information relating to an identified or identifiable natural person (Data Subject) included in the Content that Provider Processes on behalf of Customer as a Data Processor in the provision of the Service. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological genetic, mental, economic, cultural, or social identity of that natural person.

1.9 **"Processing"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.10 **"Sub-processor"** means the entity engaged by the Data Processor or any further Sub-processor to Process Personal Data on behalf and under the authority of the Data Controller.

1.11 "**Supervisory Authority**" means (a) an independent public authority which is established by a member state of the European Union pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of the Applicable Privacy Laws.

1.12 "**Terms of Service"** means the Provider's Terms of Service for the use of and access to its services, software, websites (including browser extensions) and/or applications as found on https://www.wetransfer.com/legal/terms.

2. Subject of this Agreement

2.1 Scope of Data Processing. The Parties acknowledge and agree that to the extent Provider provides services to Customer to upload, share, preview, organize, create, present or otherwise process Content which contains Personal Data, Provider acts on behalf of Customer and is Processing Personal Data in accordance with this Agreement. FOR THE AVOIDANCE OF DOUBT, PERSONAL DATA WHICH ARE NOT PART OF THE CONTENT, INCLUDING BUT NOT LIMITED TO CUSTOMER'S ACCOUNT DETAILS, ACCOUNT DETAILS OF TEAM MEMBERS OF CUSTOMER, CUSTOMER'S EMAIL ADDRESS(ES), EMAIL ADDRESS(ES) OF RECIPIENTS AND TEAM MEMBERS, PAYMENT DETAILS, DEVICE DATA AND METADATA ARE NOT SUBJECT TO THIS AGREEMENT. WETRANSFER ACTS AS INDEPENDENT DATA CONTROLLER REGARDING THOSE PERSONAL DATA.

2.2 This DPA replaces all prior data processing agreements between the Parties about the Processing of Personal Data.

2.3 Where the provisions of this Agreement contradict the Contract in relation to the Processing of Personal Data, the provisions of this Agreement prevail unless otherwise expressly provided in this Agreement.

2.4 Following this Agreement, Provider Processes Personal Data on behalf of Customer and under Customer's responsibility.

2.5 Provider Processes Personal Data exclusively for the purposes following execution of the Contract.

2.6 Provider will Process Personal Data only in accordance with the instructions of Customer. Provider has no independent control of Personal Data that it Processes on behalf of Customer. Provoder may not Process Personal Data for its own benefit, the benefit of third parties or other purposes, except with Customer's prior written consent or where required by law.

2.7 Customer acknowledges and agrees that Provider shall Process Personal Data to monitor, prevent, detect, block and delete Illegal Content.

2.8 Provider shall not "sell" or "share" Personal Data, as those terms are defined under the Applicable Privacy Laws.

2.9 If Provider is required by law to disclose or otherwise Process Personal Data that is not in accordance with the instructions of the Customer, the Provider will inform the Customer of these requirements prior to Processing the Personal Data, unless that law prohibits such information.

3. Obligations of Data Controller

3.1 It's Customer's responsibility to provide written instructions to Provider. Customer warrants that any instructions it provides are in accordance with Applicable Privacy Laws.

3.2 Customer is responsible for assessing and ensuring that the Processing of Personal Data is legitimate.

3.3 Verbal instructions issued by Customer to Provider must be confirmed in writing without delay, but in any case no later than 5 working days after providing the verbal instructions.

3.5 Customer is responsible for responding within the timeframes defined in the Applicable Privacy Laws to enquiries, requests and complaints of Data Subjects in accordance with article 10 of this Agreement.

4. Confidentiality

4.1 Provider shall keep Personal Data confidential and shall not disclose Personal Data in any way to its employees or subcontractors, and/or third parties, except where, (i) it is necessary that employees, subcontractors and/ or third parties gain access to Personal Data for the purpose of execution of the Contract, or (ii) it is required by law.

4.2 Provider shall provide its employees, subcontractors and/or third parties access to Personal Data only to the extent necessary to perform the processing activities, as required for the execution of the Contract. Provider ensures that persons authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.3 In this Agreement "Confidential Information" means all information disclosed (whether in writing, orally, or electronically, or whether directly or indirectly) by the Provider to the Customer whether before, on, or after the effective date of this Agreement. This includes, without limitation,

information relating to the disclosing party's products and services, operations, customers, members, prospects, know-how, design rights, trade secrets, market information, data privacy & security information, business affairs and any communication, documentation and other information related to the (process of) data protection impact assessments, audits and inquiries, including, but not limited to, the preparation, findings, conclusions and recommendations.

4.4 Customer shall keep the Confidential Information under this Agreement confidential and may not disclose the Confidential Information to any third party. The restrictions imposed by this Section shall not apply to the disclosure of the Confidential Information:

a) which is now in, or hereafter comes into the public domain otherwise than by the Customer's breach of this section;
b) which is required by law, governmental, regulatory or court order ("Legal Order") to be disclosed;
c) which is already known to the Customer otherwise than as a consequence of a breach of this section;
d) which is received from a third party without similar restrictions and without breach of this section;
e) which is independently developed or acquired by the Customer or their associated companies independently of anything provided by the other party; or
f) which is approved for release by written authorization from the Provider.

4.5 All the obligations of the Customer pursuant to this Agreement shall survive with respect to any Confidential Information received prior to expiration or termination of this Agreement for a period of 5 (five) years from the date of disclosure of such Confidential Information.

5. Sub-processors

5.1 Customer authorizes and consents to Provider engaging Sub-processors to Process Personal Data under this Agreement. Provider will: (i) provide Customer with such details about the Sub-processor(s) it uses as may be reasonably requested by Customer from time to time; (ii) ensure that Sub-processors are contractually bound to the equivalent obligations with respect to the Processing as those which Provider is bound to under this Agreement. Information about the Sub-processors that Provider uses is available on the Provider's website and may be updated by Provider from time to time in accordance with this Agreement.

5.2 Provider shall make available on its website a list of the Sub-processors it uses (an up-to-date list is currently provided here) and shall update the list to reflect any addition or replacement to Sub-processors. Customer shall periodically check the list and may reasonably object to the use of a new Sub-processor on legitimate grounds, subject to the termination and liability clauses of the Contract. Customer acknowledges that these Sub-processors are essential for the execution of the Contract and that objecting to the use of a Sub-processor may prevent Provider from executing the Contract.

5.3 The Parties agree that if copies of the Sub-processor agreements must be sent by Provider to the Customer pursuant to the Applicable Privacy Laws, such copies may have all commercial information and clauses unrelated to this Agreement removed by Provider beforehand; and, that such copies will be provided by Provider only upon reasonable request by Customer.

6. Transfer of Personal Data

6.1 Customer agrees that Provider, its affiliates, and any Sub-processors engaged by Provider may transfer Personal Data processed under this Agreement outside the European Economic Area ("EEA"), the UK or Switzerland as necessary to provide the Service. If Provider transfers Personal Data protected under this Agreement to a jurisdiction for which the European Commission has not issued an adequacy decision, Provider will ensure that appropriate safeguards, such as the most recent EU Standard Contractual Clauses, have been implemented for the transfer of Personal Data in accordance with the Applicable Privacy Laws.

7. Security, data breaches and DPIA

7.1 Provider agrees to implement at least the technical and organizational 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 Contract.

7.2 Upon receiving knowledge of a security incident (e.g. a security breach) or data breach of Customer's Personal Data, Provider will notify Customer without undue delay.

7.3 With respect to each security incident referred to in article 7.2, Provider shall provide all assistance to Customer that can reasonably be expected of Provider, including the provision of adequate information regarding the incident., inquiries from authorities, limiting the impact of a security incident on the privacy of the Data Subject(s) and/or limiting Customer's damage as a result of the security incident.

7.4 Provider will regularly evaluate its security measures with regard to Personal Data Processing.

7.5 Provider shall provide reasonable assistance to Customer with any relevant data protection impact assessments, and prior consultation, including, if applicable and available by (a) making available for review copies of the (internal and external) (summaries of) the audit reports or other documentation describing relevant aspects of Provider's information security program and the security measures applied in connection therewith; and (b) providing a description of the processing of Content undertaken by Provider.

8. Right to audit

8.1 In order to assist Customer in demonstrating compliance with GDPR and at Customer's reasonable written request, Provider will make available to Customer the necessary information, including the most recent relevant (internal or external) assessments, audit reports or summaries and certifications, where applicable and available.

8.2 If Customer reasonably believes further information is necessary in order to confirm Provider's compliance with the provisions of the Agreement relating to Personal Data subject to the Applicable Privacy Laws, Provider will use reasonable efforts to respond to written questions by Customer regarding the information provided under 8.1.

8.3 If Customer is not satisfied with Provider's responses to questions provided pursuant to section 8.2, Provider will permit Customer to conduct an audit or inspection of Customer's processing systems and facilities strictly necessary to the extent relevant to the Processing of Personal Data

in relation to Customer's instructions. Provider will provide reasonable and necessary cooperation to such audits.

8.4 Audits shall be performed during Provider'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 30 days in advance. Customer shall ensure minimal disruption to the business of Provider. Upon Provider's request, Customer shall provide a copy of the audit report to Provider.

8.5 Customer shall bear the full costs of any audit that is requested, including any costs in time and resources made by Provider due to the request.

9. Inspection or audits by Supervisory Authority

9.1 Provider shall submit its relevant processing systems, facilities and supporting documentation to an inspection or audit relating to the Processing by a competent Supervisory 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 Supervisory Authority deems the Processing in relation to the Agreement unlawful, the parties shall take immediate action to ensure future compliance with the Applicable Privacy Laws.

10. Cooperation enquiries & Data Subject rights

10.1 Provider shall promptly forward complaints, requests or enquiries received from Data Subjects. Provider shall not respond to Data Subjects directly. Customer is solely responsible for responding to Data Subjects.

11. Government agency requests

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

11.2 Provider shall inform Customer of a government agency request to provide (access to) Personal Data, unless the law or the government agency request expressly prohibits such notification.

12. Costs and Liability

12.1 The execution costs of this Agreement are included in the prices and fees as agreed upon in the Contract.

12.2 The total liability of either Party and its affiliates towards the other Party and its affiliates, whether in contract, tort or any other theory of liability, under or in connection with this Agreement will be limited to limitations on liability or other liability caps agreed to by the parties in the Contract.

13. Indemnity

13.1 Customer will defend, indemnify and hold harmless Provider (including its employees and affiliates) from and against any claims, incidents, liabilities, procedures, damages, losses and expenses (including legal fees), arising out of or in any way connected with Customer's access to or use of the Service or Customer's breach of this Agreement, including any third party claims that the Content created, used, stored or shared using the services by Customer or through Customer's account, infringe or violate any third party rights.

14. Return and deletion of Personal Data

14.1 Upon termination of the Agreement, Provider shall, at the choice of Customer, delete and/or return Personal Data, except to the extent the Agreement or applicable laws provide otherwise. In that case, Provider shall no longer process the Personal Data, except to the extent required by the Agreement or applicable laws. Customer may require Provider to confirm and warrant that Provider has deleted and/or destroyed all copies of the Personal Data. Customer shall reimburse Provider for any additional costs arising from the return of the Personal Data.

14.2 No Backups. Provider's Service do not include backup services or disaster recovery Customer's Content.

15. Term and termination

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

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

16. Changes and Renegotiations

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

16.2 The Agreement will only be valid while Customer follows and adheres to the accompanying Contract.

17. Miscellaneous

17.1 This Agreement and any non-contractual obligations arising out of or in connection with it will be governed by and construed and interpreted in accordance with Dutch law.

17.2 Any disputes regarding this Agreement will be submitted to the exclusive jurisdiction of the competent court of Amsterdam (The Netherlands).

17.3 Any standard terms of business and other standard or special terms and conditions of Customer do not apply to this Agreement and are explicitly dismissed by Provider.

Technical and organizational security measures

Provider protects Customer's data according to those standards.

1. **Data Access Controls:**
   Provider ensures that Personal Data is accessible and manageable only by properly authorized staff who need access to perform their tasks, direct database query access is restricted and activity by those who have access is 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 authorized staff in the course of Processing.

2. **Transmission Controls:**
   Provider ensures that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport from Customer to Provider. Transfers are encrypted when they are uploaded, downloaded and while they are hosted on the server of Provider, and only sent over a secured (https) connection while they are transported from Customer to Provider and back.

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

4. **Sub-processor Security:**
   Before onboarding new Sub-processors, Provider 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 to take measures to maintain appropriate safeguards, such as signing standard contractual clauses (SCCs).

5. **Personnel Security:**
   Provider'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. Provider's staff is required to execute a confidentiality agreement and is provided with privacy and security training.

6. **Logical Separation:**
   Personal Data from different Provider's subscriber environments is logically segregated on Provider'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.