WeTransfer Data Processing Agreement

Last update: November, 2025

This Data Processing Agreement ("**DPA**") is entered into between the Customer, as defined in the Agreement ("**Customer**"), and WeTransfer B.V., with registered office at Nieuwezijds Voorburgwal 162, 1012 SJ, Amsterdam, the Netherlands ("**WeTransfer**" or "**Provider**"). The Customer and the Provider may be referred to herein individually as the "**Party**" and collectively as the "**Parties**".

Whereas:

A. The Customer entered into the Provider's Terms of Service or any other agreement with the Provider ("**Agreement**") according to which the Provider will provide services to the Customer ("**Service**").

B. To provide the Service, the Provider will process personal data as a data processor on behalf of the Customer.

C. The Parties agree that clauses 2 to 10 of this DPA apply to any processing of personal data carried out by the Provider as data processor. The processing activities and personal data processed by the Provider on behalf of the Customer are described in Annex I of this DPA.

D. The Parties agree that clause 11 of this DPA applies to the processing operations carried out by WeTransfer in its role as autonomous data controller and for its own purposes (as better described in clause 11 of this DPA).

E. The Parties enter into this DPA, which is hereby incorporated into the Agreement, in order to ensure that they comply with Applicable Privacy Law (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 DPA, the following terms have the following meanings.

1.1 "**Adequacy Decision**" means a legally binding decision issued by the European Commission, allowing the transfer of Personal Data from the EEA to a third country that has been considered adequate in terms of data protection safeguards.

1.2 "**Agreement**" as defined in recital A.

1.3 "**Applicable Privacy Law**" means all applicable data protection laws and regulations, including but not limited to Regulation (EU) 2016/679 ("**GDPR**") and the California Consumer Privacy Act at Cal. Civ. Code § 1798.100 et seq., and its implementing regulations ("**CCPA**").

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

1.5 “**Data Controller**” means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

1.6 “**Data Processor**” means the entity that processes Personal Data on behalf of the Data Controller.

1.7 **“Data Subject”** means an identified or identifiable natural person to which the Personal Data pertains**.**

1.8 “**Data Subjects’ Rights**” means the rights which Data Subjects are entitled to under the Applicable Privacy Law, including but not limited to the right to request access to, rectification or erasure of Personal Data, to request the restriction of Processing concerning the Data Subject or to object to Processing, as well as the right to data portability.

1.9 “**EEA**” means the European Economic Area**.**

1.10 “**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.

1.11 “**Personal Data**” means information that the Data Processor processes on behalf of the Data Controller that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to a Data Subject.

1.12 “**Personal Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

1.13 **“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**.**

1.14 **“Service”** means the services and activities regulated by the Agreement.

1.5 **“Standard Contractual Clauses”** means the standard contractual clauses adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 of 4 June 2021, on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, and available at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN.

1.16 “**Sub-processor**” means an entity engaged by the Data Processor to assist it in (or who undertakes any) processing of Personal Data in the performance of the Data Processor’s obligations pursuant to the DPA.

1.17 “**Transfer Mechanisms**” means an Adequacy Decision issued by the European Commission allowing the transfer of personal data from the EEA to a third country whose domestic law provides an adequate level of protection of personal data. Where such Adequacy Decision is not available or effective, this definition means the Standard Contractual Clauses, as well as binding corporate rules (BCRs) approved by a competent Supervisory Authority.

2. Obligations of the Customer

2.1. The Customer agrees that in order for the Provider to provide the Service, the Customer shall provide the Provider with Personal Data.

2.2. The Customer is responsible for assessing and ensuring that the Processing of Personal Data is legitimate and in compliance with Applicable Privacy Law.

2.3. The Customer represents and warrants that it has an appropriate legal basis to process and disclose Personal Data to the Provider as part of the provision of the Service.

2.4. The Customer represents and warrants that it fully complies with the Applicable Privacy Law, indemnifying the Provider against all damages, costs, and losses incurred as a result of any breach by the Customer of the provisions of the Applicable Privacy Law.

2.5. It’s the Customer’s responsibility to provide written instructions to the Provider. The Customer warrants that any instructions it provides are in accordance with the Applicable Privacy Law. Verbal instructions issued by the Customer to the Provider must be confirmed in writing without delay, but in any case no later than 5 working days after providing the verbal instructions.

3. Obligations of the Provider

The Provider agrees to:

3.1. Ensure the confidentiality of the Personal Data that learns or becomes aware of in the performance of the Service or the Agreement and comply with the instructions given by the Customer.

3.2. Process Personal Data only in accordance with the instructions of the Customer, unless required by law to do otherwise. The Customer acknowledges and agrees that Provider shall process Personal Data to monitor, prevent, detect, block and delete Illegal Content.

3.3. Except as otherwise expressly permitted by Applicable Privacy Law, not retain, use, disclose, or otherwise process Personal Data for any purpose other than those specified in the Agreement or this DPA.

3.4. Limit Personal Data collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the processing set out in this DPA and the Agreement and not process the Personal Data in a manner incompatible with those purposes.

3.5. To the extent the CCPA applies to the processing of Personal Data, unless otherwise permitted by Applicable Privacy Law, the Provider shall not: (i) “sell” or “share” Personal Data within the meaning of the CCPA, and (ii) retain, use, or disclose Personal Data (a) for any purpose other than to perform, support, and improve the Service, or (b) outside of the direct business relationship between Provider and the Customer. The Provider shall notify the Customer if the Provider determines that it can no longer meet its obligations under the CCPA.

3.6. In accordance with Applicable Privacy Law, implement adequate operational, technical and organisational measures to ensure the confidentiality, integrity, and availability of Personal Data

and to eliminate or, in any case, to minimize any risk of destruction or loss of data, whether or not accidental, and of unauthorized or non-compliant processing, taking into account (1) the current state of the art and technical progress, (2) the risks associated with the data processed, and (3) the nature of the data. These measures are listed in Annex 2 of this DPA.

3.7. Cooperate with and assist the Customer in ensuring its compliance with its obligations under Applicable Privacy Law, including but not limited to assisting with data protection impact assessments, audits, and consultations with regulatory bodies, taking into account the nature of the Processing and the information available to the Provider.

3.8. Provide the personnel authorized to process Personal Data with instructions on the operations to perform in compliance with the Provider's obligations under this DPA, ensuring that the instructions given are duly observed, and the authorized personnel are under an appropriate obligation of confidentiality.

3.9. Cooperate in good faith with the Customer to ensure compliance with this DPA, assist the Customer in complying with its obligations under the Applicable Privacy Law, and make available to the Data Controller all information necessary to demonstrate compliance with the Applicable Privacy Law.

3.10. Notify the Customer, unless legally prohibited from doing so, after having become aware of any communication with the relevant Supervisory Authority, courts, law enforcement authorities, or other public authorities in relation to the Processing of Personal Data regulated by this DPA.

3.11. Immediately inform the Customer when, in the Provider's opinion, an instruction received from the Customer violates the Applicable Privacy Law.

3.12. Assist the Customer with appropriate technical and organizational measures to comply with all Data Subjects' Rights requests that the Customer may receive, pursuant to Clause 6 of this DPA.

3.13. Appoint a data protection officer, where required by Applicable Privacy Law.

4. Authorization for Sub-processing

4.1. The Customer acknowledges, agrees, and consents that, for the sole and exclusive purpose of providing the Service and subject always to compliance with the terms of this DPA, Personal Data may be processed by the Provider and its Sub-processors.

4.2. The Customer hereby authorizes the Provider to engage Sub-processors subject to the conditions that the Provider:

i. enters into a written agreement with the Sub-processor containing the same obligations as set out in this DPA or, in any case, ensures that the Sub-processor offers no fewer guarantees than those offered by the Provider in this DPA;

ii. assesses the Sub-processor and remains liable for the actions or omissions of the Sub-processor with regard to its obligations under this DPA;

iii. makes available a list of the Sub-processors upon request of the Customer and at the following link (https://wetransfer.com/it-IT/explore/legal/services-subprocessors). The Provider will update the list to reflect any additions or replacements to Sub-processors and will provide reasonable notice to the Customer of the engagement of any new Sub-processor. The Customer must subscribe to receive such notice of updates to the list of Sub-processors using the link above.

4.3. The Customer may reasonably object in writing to the use of a new Sub-processor within ten (10) calendar days of notice, provided that such objection is based on reasonable grounds relating to

data protection, and subject to the termination and liability clauses of the Agreement. In the event of an objection, the Provider and the Customer will discuss such concerns in good faith. The Customer acknowledges that the Sub-processors are essential for the provision of the Service and that objecting to the use of a Sub-processor may prevent the Provider from offering the Service to the Customer.

5. Transfers of Personal Data

5.1. If the Customer is an EEA-based Customer, and the provision of the Service entails the transfer of Personal Data from the EEA to a country located outside the EEA, the Parties will rely on an Adequacy Decision issued by the European Commission. Where such Adequacy Decision is not available or effective, the Parties agree that the Standard Contractual Clauses are incorporated into this DPA by reference and will apply to those transfers.

5.2. To the extent that Standard Contractual Clauses apply between the Customer and the Provider, the Parties agree upon the following:

i. only the clauses of the Standard Contractual Clauses under MODULE TWO or MODULE THREE will apply (as applicable)

ii. Clause 7 of the Standard Contractual Clauses is applicable

iii. under Clause 9(a) of the Standard Contractual Clauses, Option 2 is applicable, under the terms of Clause 4 of this DPA

iv. the optional clause under Clause 11(a) of the Standard Contractual Clauses is not applicable

v. under Clause 17 of the Standard Contractual Clauses, Option 1 is applicable. The laws of the Netherlands will apply

vi. under Clause 18(b) of the Standard Contractual Clauses, any disputes regarding this Agreement will be submitted to the exclusive jurisdiction of the competent court of Amsterdam (The Netherlands)

vii. Annex 1 of the Standard Contractual Clauses shall be deemed completed with the information included in Annex 1 of this DPA

viii. Annex 2 of the Standard Contractual Clauses shall be deemed completed with the information included in Clause 3.6 of this DPA

ix. Annex 3 of the Standard Contractual Clauses shall be deemed completed with the information included in Clause 4.2 of this DPA.

5.3. To the extent that the transfer of Personal Data outside the EEA only occurs between the Provider and a Sub-processor, the Provider commits to entering into the Standard Contractual Clauses with that Sub-processor and only the clauses under MODULE THREE: Transfer processor to processor will apply (to the exclusion of the other MODULES).

6. Data Subjects' Rights

6.1. Taking into account the nature of the processing, the Provider will assist the Customer in the fulfilment of the Customer's obligations, under the Applicable Privacy Law, to respond to requests to exercise Data Subjects' Rights, by means of appropriate technical and organizational measures.

6.2. The Provider will cooperate with and assist the Customer, in responding to Data Subjects' Rights requests in a timely and lawful manner, and provide such information as may reasonably be

required to respond to Data Subjects' Rights, or otherwise to enable the Customer to comply with its duties related to Data Subjects' Rights under the Applicable Privacy Law.

6.3. In the event the Provider receives a request directly from a Data Subject relating to Personal Data, the Provider will immediately notify the Customer, and at the Customer's direction, act on behalf of the Customer in accordance with the Customer's instructions for responding to such requests.

7. Right to audit

7.1. At the Customer's written request, the Provider will provide the Customer with all the relevant and reasonable information in the form of documentation to demonstrate the Provider's compliance with its obligations set forth in this DPA.

7.2. Should the Customer show that the documents and information provided do not sufficiently demonstrate the Provider's compliance, the Provider will allow for and contribute to an audit conducted by the Customer by making available to the Data Controller additional documents and information reasonably requested that demonstrate the Provider's compliance with its obligations set forth in this DPA.

7.3. An audit shall be performed during the 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 90 (ninety) days in advance. The Customer shall ensure minimal disruption to the business of the Provider. Upon the Provider's request, the Customer shall provide a copy of the audit report to the Provider.

7.4. Any information gathered on the Provider's activities will be subject to a specific confidentiality agreement between the Parties.

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

8. Personal Data Breach

8.1. Upon receiving knowledge of a Personal Data Breach of the Customer's Personal Data, the Provider will notify the Customer without undue delay.

8.2. With respect to each Personal Data Breach, the Provider shall provide all assistance to the Customer that can reasonably be expected of the Provider, including the provision of adequate information regarding the breach, inquiries from authorities, limiting the impact of the breach and the Customer's damage as a result of the breach.

8.3. The Provider shall promptly adopt adequate corrective measures to remedy a Personal Data Breach and shall cooperate with the Customer to develop and implement an action plan to address the Personal Data Breach in accordance with Applicable Privacy law.

9. Liability and Indemnity

9.1. In the event of breach of this DPA by the Provider, the Customer will be entitled to withdraw from the Agreement at no cost and without penalties, unless the Provider adopts the corrective measures required by the Customer.

9.2. The Provider agrees to maintain sufficient financial and personnel resources to fulfill its obligations arising from the DPA.

9.3. The Customer shall defend, indemnify and hold harmless the 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 the Customer's access to or use of the Service or the Customer's breach of this DPA, including any third party claims that the Content created, used, stored or shared by the Customer using the Service or through the Customer's account infringes or violates any third party rights.

10. Return and Deletion of Personal Data

10.1. Three years after the last use of the Service or the expiration of the subscription, as defined in the Agreement, whichever occurs later, the Provider shall delete the Personal Data, except to the extent that the Agreement or applicable laws state otherwise. Upon the Customer's request, the Provider shall offer a means for the Customer to retrieve the Personal Data prior to such deletion.

10.2. The Customer shall reimburse the Provider for any additional costs arising from the return of the Personal Data.

11. Further processing carried out as an autonomous Data Controller

11.1. The Customer acknowledges that personal data involved in the Service which are not part of the Content, including but not limited to the Customer's account details, account details of team members of the Customer, the Customer's email address(es), email address(es) of recipients and team members, payment details, device data and metadata, are processed by WeTransfer for the following autonomous further purposes in its quality as autonomous Data Controller: (1) establish, exercise, or defend rights of WeTransfer and its affiliates, including proving the correct execution of the Service, (2) comply with legal or regulatory obligations applicable to the processing and retention of data to which WeTransfer is subject, (3) ensure and improve the quality and the proper functioning of the Service, including by analyzing, preventing or correcting failures and bugs, as well as the illicit use or misuse of the Services, and (4) enforce the Agreement and enhance the safety and integrity of the Service.

11.2 For any communication and request regarding the processing operations carried out according to this clause, WeTransfer can be reached at privacy-wetransfer@bendingspoons.com.

11.3. When clause 11.1. applies, the Customer and WeTransfer undertake to process the personal data in accordance with Applicable Privacy Law. In particular, the Customer and WeTransfer will be liable to make sure they have a legal basis for collecting and processing the personal data, will provide transparent information to data subjects about the processing as well as carry out any other assessment or actions required by the Applicable Privacy Law.

12. Miscellaneous

12.1. All communications relating to this DPA and privacy matters, directed to the Provider, must be addressed to the contacts specified in Annex I of this DPA. All communications related to this DPA and privacy matters, directed to the Customer, must be addressed to the email address provided by the Customer during the subscription to the Agreement. Each Party will notify the other of any update in its contact details.

12.2. This DPA will remain in effect for the term of the Agreement and, in any event, during the performance of the Service, in which case it will terminate upon completion of the Service, subject to Clause 10 (Return and Deletion of Personal Data).

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

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

12.5. All provisions in this DPA are an integral part of the general relationship between the Customer and the Provider. The performance of this DPA will not result in the recognition of any specific consideration, remuneration, indemnification, compensation or reimbursement in favor of the Provider in addition to that established in the Agreement.

12.6. In the event of a conflict between the terms of this DPA and the Agreement, this DPA will prevail.

ANNEX I - Description of Processing where the Provider acts as a Data Processor

A. LIST OF PARTIES

Data exporter: Customer

Name: Name as listed in the Customer's account.

Address: Address as listed in the Customer's account.

Contact person: Account owner listed in the Customer's account.

Activities relevant to the data transferred under these Clauses: Activities described in Section B. below.

Role (controller/processor): Data Controller

Data importer: Provider

Name: WeTransfer B.V.

Address: Nieuwezijds Voorburgwal 162, 1012 SJ, Amsterdam, the Netherlands

Contact person: DPO or Privacy Counsel, privacy-wetransfer@bendingspoons.com

Activities relevant to the data transferred under these Clauses: Activities described in Section B. below.

Role (controller/processor): Data Processor

B. DESCRIPTION OF PROCESSING AND TRANSFER

Categories of data subjects whose personal data is transferred

Customer's employees, Data Subjects mentioned or represented in the Content.

Categories of personal data transferred

Any Personal Data included in the Content.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

On a continuous basis through the use of the Service.

Nature of the processing

The Provider will process the Personal Data only for the purpose of providing the Service to the Customer.

***Purpose(s) of the data transfer and further processing*:**

Provision of the Service.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal Data that is not part of the Content will be retained as long as the Customer remains active, and for 3 years after that moment. The Content will be deleted automatically and permanently from the Provider's servers within 48 hours after expiration, unless the transfer is set to "Recoverable," in which case it will be deleted one (1) year after expiration. The Customer can delete the Content at any time.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Sub-processors are employed to receive support for the provision of the Service.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in accordance with Clause 13 of the Standard Contractual Clauses is the Dutch "Autoriteit Persoonsgegevens."

ANNEX II - Technical and organizational security measures

The Provider protects the Customer's data according to those standards.

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

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

4. **Sub-processor Security:**
   Before onboarding new Sub-processors, the 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:**
   The 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 the different Provider's subscriber environments is logically segregated on the Provider's systems to ensure that Personal Data that is collected for different purposes may be processed separately.

7. **Erasure of transfers:**
   The Content, including any Personal Data that is part of the Content, is permanently deleted from the Provider's servers within 48 hours after expiration, unless the transfer is set to "Recoverable," in which case it is deleted 1 year after expiration. This means there is no way to retrieve the Content of a transfer after its deletion.