



SCREENCASTIFY DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is effective as of the date fully signed below, as indicated in the Order Form to which it is attached, or as indicated in other online terms through which this DPA is incorporated ("**Effective Date**") and is entered into between the customer identified in the Order Form or other online terms through which this DPA is incorporated or as indicated in the signature line below ("**Customer**") and Screencastify, LLC with an address at 333 N. Green St., Suite 810, Chicago, IL 60607 ("**Screencastify**" or "**Provider**"). This DPA forms part of the (i) Order Form to which it is attached or incorporated into or (ii) other online terms through which this DPA is incorporated that have been entered into between Customer and Provider ("**Agreement**"), under which Provider has agreed to provide to Customer certain software services ("**Services**").

In performing the Services, Provider may be required to process certain Personal Data that is subject to the EU General Data Protection Regulation and UK General Data Protection Regulation ("**GDPR**"); the Australian Privacy Act 1988 ("**AU Privacy Act**"); the New Zealand Privacy Act 2020 ("**NZ Privacy Act**"); the Brazilian General Data Protection No. 13,709/2018 ("**LGPD**"); and all applicable data protection laws in the United States, including but not limited to, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, Colorado Privacy Act, Connecticut Act Concerning Personal Information Privacy and Online Monitoring, Virginia Consumer Data Protection Act, and Utah Consumer Privacy Act and implementing regulations of all such laws, whether such laws are in place as of the Addendum Effective Date or come into effect during the term (all of the foregoing laws collectively referred to herein as, "**Applicable Laws**").

How to Execute this DPA

1. This DPA consists of the main body of the DPA including Exhibit A and Exhibit B.
2. This DPA has been pre-signed on Screencastify's behalf as the data importer.
3. To complete this DPA, Customer must complete the information in the signature box and sign on page 7 and return to Screencastify at legal@screencastify.com.

Where Customer and Screencastify are parties to an Agreement and upon Screencastify's receipt of a completed DPA in accordance with the instructions above, this DPA will become legally binding. For the avoidance of doubt, signature on page 7 of this DPA shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated into this DPA by reference

DPA Terms

1. **Definitions.** The capitalized terms in this DPA shall have the meanings set forth below and otherwise throughout this DPA. Any capitalized terms not defined herein shall have the meanings set forth in the Agreement.

"**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**" and "**Supervisory Authority**" shall have the same definitions as set forth under Applicable Laws.

“Service Provider” and **“Business”** have the meaning given in Applicable Laws.

"Affiliate" means an entity of a party, whether incorporated or not, that controls, is controlled by, or is under common control with such party, where "control" means the ability, whether directly or indirectly, to direct the affairs of another by means of ownership, contract or otherwise.

"EEA" means the European Economic Area.

"Member State" refers to a country that is a member of the European Economic Area.

"Subprocessor" means any other Processor that is engaged by Provider (e.g. such as an Affiliate or subcontractor) for the performance of the Services on behalf of the Controller.

2. **Scope.** This DPA governs each party's respective rights and obligations with respect to the Processing of Personal Data pursuant to Applicable Laws.
3. **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data under this DPA, Customer is the "Controller" or “Business” and Provider is the "Processor” or “Service Provider.”
4. **DPA Term, Details of Processing, & Duration of Processing.** This DPA begins on the Effective Date and will end coterminous with the Agreement. Any terms and conditions herein that by their nature are intended to survive the termination or expiration of this DPA shall survive. Details of the Processing by Provider are attached hereto as Exhibit A. Provider will Process Personal Data until the earlier of: (1) the Agreement is terminated or expires, or (2) until notified in writing by Controller to discontinue Processing Personal Data.

5. Rights and Obligations of Customer

- a. Compliance with Applicable Laws. Customer shall comply with Applicable Laws.
- b. Lawful Means For Processing. Customer is responsible for ensuring that it has a lawful means for Processing Personal Data under Applicable Laws. Customer represents and warrants that it will obtain any and all necessary consents from data subjects prior to transferring the Personal Data to Provider. Customer shall indemnify, defend and hold harmless Provider and its Affiliates for any claims, suits, damages, losses, liabilities, fines, penalties, attorneys' fees and court costs that Provider incurs arising from Customer's violation of Applicable Laws.
- c. The Means for Processing. Customer has the right and the obligation to determine the purposes for which Personal Data is Processed by Provider.

6. Obligations of Provider

- a. **Processing of Personal Data.** Personal Data is being provided to Provider for a limited and specified purpose, and Provider is prohibited from processing Personal Data for any purpose other than the specific purpose of performing the Services specified in the Agreement. Provider (i) shall comply with applicable obligations under Applicable Laws and shall provide at least the same level of privacy protection to Personal Data as is required by this Agreement and Applicable Laws; (ii) agrees that Customer has the right to take reasonable and appropriate steps to help to ensure that Provider's use of Personal Data is

consistent with Customer's obligations under this DPA and Applicable Laws; (iii) shall notify Customer's in writing of any determination made by Provider that it can no longer meet its obligations under this DPA or Applicable Laws; and (iv) agrees that Customer's has the right, upon notice, including pursuant to the preceding clause, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

- b. No Sale of Personal Data. Customer and Provider hereby acknowledge and agree that in no event shall the transfer of Personal Data from Customer to Provider constitute a sale of Personal Data or transfer of Personal Data for valuable consideration to Provider, and that nothing shall be construed as providing for the sale or transfer for valuable consideration of Personal Data to Provider. Provider shall not (and will require that its subcontractors do not): (i) sell or share Personal Data; (ii) retain, use, or disclose Personal Data received from or on behalf of Customer for a commercial purpose that is not necessary to provide the Services; (iii) retain, use, disclose, release, transfer, make available, or otherwise communicate Personal Data outside of the direct business relationship between Customer and Provider; or (iv) combine Personal Data with Personal Data that Provider receives from or on behalf of another business or person, or that it collects from its own interactions with individuals.
- c. Processing on Written Instructions. Provider shall only Process Personal Data on the express written instructions of Customer, including with regard to the transfer of Personal Data to a third country, unless otherwise required by Applicable Laws. For the avoidance of doubt, providing the Services as expressly set forth in the Agreement constitutes complying with Customer's written instructions. Where Provider is relying on Applicable Laws as the basis for Processing Personal Data, Provider shall promptly notify Customer of such Processing prior to Processing unless Applicable Laws prohibit such prior notice.
- d. Data Protection Officer. Where required by Applicable Laws, Provider shall designate and maintain a data protection officer responsible for monitoring and ensuring compliance with Applicable Laws.
- e. Notice of Violation of Law. Provider shall immediately notify Customer if, in Provider's opinion, any instruction given by Customer violates Applicable Laws ("**Challenged Instruction**"). The parties will work together in good faith to promptly address any Challenged Instruction.
- f. Duty of Confidentiality. Provider shall ensure that all persons processing Personal Data on its behalf, including Provider's and its Subprocessor's employees, agents and contractors, are subject to a duty of confidence or are under an appropriate statutory obligation of confidentiality.
- g. Appropriate Security Measures. Before Processing Personal Data on behalf of Customer, Provider shall implement technical and organizational measures to ensure a level of security appropriate to the risk. Provider shall consider the following when implementing such security measures, as appropriate: (i) 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;

and (iv) a process for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures for ensuring the security of the Processing.

- h. Records and Audits. Provider shall maintain complete and accurate records regarding the Processing it performs under the Agreement and this DPA, including as necessary to demonstrate its compliance with the data privacy and security obligations of the DPA and Applicable Laws. Provider shall promptly provide Customer with such aforementioned records and information upon reasonable request. Upon request, Provider shall permit Customer or its designated agent to audit any such records and perform any such other audits required in order for Customer to establish both Customer's and Provider's compliance with Applicable Laws.
- i. Notice Requirements.
 - i. Government Request. Provider shall notify Customer, without undue delay, of any request for disclosure of Personal Data by law enforcement or governmental authorities, unless prohibited by Applicable Laws.
 - ii. Data Subject Request. Provider shall notify Customer, without undue delay, of any complaints or requests received from a Data Subject, such as requests for access, rectification, erasure, restriction of Processing, data portability, objection to Processing, or objection to automated-decision making. If Provider receives any such requests, Provider shall not respond to the Data Subject directly unless authorized to do so by Customer or required by Applicable Laws, but shall instead permit Customer to respond directly to the Data Subject.
 - iii. Notice of a Personal Data Breach. Provider shall, without undue delay and within the period specified by Applicable Laws, notify Customer of any known Personal Data Breach.
- j. Assistance. Taking into account the nature of the Processing relating to Provider's services and the information available to Provider, Provider shall assist Customer in meeting Customer's obligations, by having appropriate technical and organizational measures, under Applicable Laws, including but not limited to:
 - i. Article 32 (Security of Processing) of the GDPR to keep data secure;
 - ii. Article 33 (Notification of personal data breach to the supervisory authority) of the GDPR to notify the Supervisory Authority of a Personal Data Breach;
 - iii. Article 34 (Communication of a personal data breach to the data subject) of the GDPR to advise Data Subjects when there has been a Personal Data Breach;
 - iv. Article 35 (Data protection impact assessment) of the GDPR to carry out data protection impact assessments ("**DPIA**"); and
 - v. Article 36 (Prior consultation) of the GDPR to consult with the supervisory authority where Customer's DPIA indicates there is an unmitigated high risk to the Processing.

- k. Personal Data Breach. In the event of a Personal Data Breach, Provider will promptly investigate such Personal Data Breach and will provide Customer with reasonable assistance to satisfy any legal obligations (including obligations to notify data protection authorities or data subjects) of Customer in relation to such Personal Data Breach.
- l. Delete and Return of Personal Data. Anytime upon request, and at the termination or expiration of the DPA, Provider shall promptly (no more than 30 days) return or delete (whichever is requested) all Personal Data Processed on behalf of Customer pursuant to this DPA, and confirm compliance with such in writing. Notwithstanding the foregoing, if Provider is required by Applicable Laws to retain any such Personal Data, Provider may retain Personal Data as required to comply with such Applicable Laws.

7. Subprocessing

- a. Using a Subprocessor. Customer generally authorizes Provider to engage Subprocessors. Provider shall use good judgment and perform due diligence on any Subprocessor used under this DPA, paying special attention to the Subprocessor's experience and the suitability of the technical and organizational measures it uses for security.
- b. Requirements of Subprocessing. Provider shall enter into a written agreement with any Subprocessor that imposes the same obligations imposed under this DPA on Provider to Subprocessor.
- c. Liability for Subprocessor. Provider is fully liable to Customer for: (i) Subprocessor's failure to comply with or fulfill its obligations under the DPA or Applicable Laws; and (ii) Subprocessor's failure to perform the Services.

8. Data subject rights

- a. Information and Assistance. Provider shall assist Customer, as reasonably requested by Customer, in enabling Data Subjects to exercise their rights under Applicable Laws. Taking into account the nature of the Processing and the information available to Provider, Provider shall provide to Customer the information and assistance required to fulfill any requests by Data Subject for access, rectification, erasure, restriction of Processing, data portability, objection to Processing, objection to automated-decision making or other rights available to Data Subjects under Applicable Laws. Customer will determine whether or not the Data Subject has the right to exercise the specific demand requested and will give specific instruction to Provider where information and/or assistance is required.

9. Cross-Border Data Transfers.

- a. Transfers Outside of the EU, EEA, and Switzerland. If Personal Data is being transferred to a recipient outside of the European Economic Area or Switzerland, then such transfers shall be governed by the EU Standard Contractual Clauses (“SCCs”), which shall be entered into and incorporated into this DPA by this reference and completed as follows:
 - i. Module 2 (Controller to Processor) will apply where Customer is a Data Controller and Provider is a Data Processor;
 - ii. Clause 7: The optional docking clause will not apply;
 - iii. Clause 9: Option 2 will apply as per the terms set out in Section 7 (Subprocessors) of this DPA;
 - iv. Clause 11: The optional language will not apply;

- v. Clause 17: Option 2 will apply, and the SCCs will be governed by the laws of Ireland in the event the law of the EU Member State in which the data exporter is established does not allow for third-party beneficiary rights;
- vi. Clause 18(b): Disputes shall be resolved by the Courts of Dublin, Ireland;
- vii. Annex 1 of the SCCs shall be deemed completed with the information set out in Exhibit A to this DPA; and
- viii. Annex 2 of the SCCs shall be deemed completed with the information set out in Exhibit B to this DPA.

Provider shall comply with its requirements under the SCCs. Nothing in this Section 9(a) is intended to conflict with either party's rights and responsibilities under the SCCs and, in the event of any such conflict, the SCCs shall prevail.

- b. **Transfers Outside of the UK.** If Personal Data is being transferred to a recipient outside of the United Kingdom, and to the extent that the Parties are lawfully permitted to rely on the SCCs for transfers of Personal Data from the United Kingdom subject to completion of the UK International Data Transfer Addendum to the SCCs issued by the Information Commissioner's Office under section 119A(1) of the Data Protection Act 2018 on March 21, 2022 ("**UK Addendum**"), the UK Addendum is incorporated herein by reference and shall be completed as follows:
 - i. In Table 1, the parties' contact information is located in Exhibit A;
 - ii. In Table 2, the selected SCCs is located in Section 9(a) of this DPA above;
 - iii. In Table 3:
 - 1. the list of parties is located in Exhibit A;
 - 2. the description of transfer is located in Exhibit A; and
 - 3. the technical and organizational measures are located in Exhibit B.
 - iv. In Table 4, both the Importer and the Exporter may end the UK Addendum in accordance with its terms (and the respective information is deemed checked).
- a. Data Transfers Outside of Australia, Brazil, and New Zealand. Customer agrees that Provider may process Personal Data outside of Australia, Brazil, and New Zealand, and represents and warrants that such transfers of Personal Data are in compliance with the AU Privacy Act, NZ Privacy Act, and LGPD.

10. Miscellaneous.

- a. Governing Law. This DPA shall be governed by the same law as set forth in the Agreement, except as otherwise required by Applicable Laws.
- b. Assignment. The assignment provision in the Agreement shall apply to this DPA as though stated herein.
- c. Change in Law. In the event of a change in Applicable Laws or in any guidance or interpretation thereof that affects the terms of this DPA, the parties agree to work in good faith to amend this DPA to address any such changes. Amendments will only be effective upon signed, written agreement of both parties.
- d. Severability. In the event a court of competent jurisdiction finds any provision of this DPA invalid or unenforceable, such provision will be interpreted to fulfill its intended purpose to the maximum extent permitted by Applicable Law, and if the foregoing is not possible,

such provision shall be severed from the Agreement. All remaining provisions shall continue in full force and effect.

- e. Waiver. Neither party shall be deemed to have waived any of its rights under this DPA by lapse of time or by any statement or representation other than by an authorized representative in an explicit signed, written waiver. No waiver of a breach of this DPA by either party will constitute a waiver of any other breach of this DPA.
- f. Counterparts. This Agreement may be executed in one or more counterparts, each of which will be an original and together all counterparts are a single instrument.
- g. Entire Agreement. Except as modified by this DPA, the Agreement shall remain in full force and effect. This DPA and the Agreement contain the entire agreement of the parties regarding the subject matter stated herein, and supersede all prior or contemporaneous negotiations, discussions, understandings or agreements between the parties relating thereto. The parties agree that any amendment to the DPA must be in writing and signed by the authorized representatives of both parties. In the event of conflict between this DPA and the Agreement, this DPA shall control with respect to the subject matter herein.

The parties execute this DPA by their authorized representatives as of the Effective Date by their signature below:

Provider

DocuSigned by:
David Pruitt
028682255AAD446...

Signature

David Pruitt

Print Name

General Counsel

Title

1/13/2023

Date

Customer

Signature

Print Name

Title

Date

Exhibit A

Processing and Transfer Details

A. LIST OF PARTIES

Controller/Data exporter:

Name:

Address:

Contact person's name, position and contact details:

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

Signature:

Date:

Processor/Data importer:

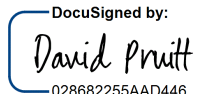
Name: Screencastify, LLC

Address: 333 N. Green St., Suite 810, Chicago, IL 60607

Contact person's name, position and contact details: privacy@screencastify.com

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

Signature and date:

DocuSigned by:

028682255AAD446...
David Pruitt
General Counsel
1/13/2023

B. DESCRIPTION OF PROCESSING AND TRANSFER

Categories of data subjects

Students and administrators of Customer

Categories of personal data

Name, e-mail address, metadata associated with use of product and any personal data contained in videos created by the data subjects

Sensitive data

None.

The frequency of processing and transfer

Personal data is processed and transferred on a continuous basis.

Nature and purpose of the processing

The nature of the Processing under the DPA includes basic Processing activities, such as storage, hosting, backup, erasure, and such other applicable Services as described in the Agreement. The purpose of processing is the provision of Services pursuant to the Agreement.

The period for which the personal data will be retained

The processing of Personal Data shall endure for the duration of the term in the Agreement and DPA.

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

The subject matter, nature and duration of the Processing shall be as specified in the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 of the SCCs

Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as the competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: the Irish Data Protection Commission shall act as the competent supervisory authority.

Where the data exporter is established in the United Kingdom, the Information Commissioner's Office shall act as the competent supervisory authority.

Exhibit B

Screencastify Security Measures

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Screencastify will undertake industry standard practices, including physical controls, firewalls, and password protection, to protect the privacy and security of Personal Data that Screencastify receives from the customer identified in this Agreement (the “Customer”), including alignment with the requirements of the National Institute for Standards and Technology (“NIST”) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Additionally, Screencastify has implemented the the following security controls intended to provide reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the PII in its custody:

- (1) Screencastify has designated a privacy officer responsible for information security governance and maintains privacy policies and practices that support compliance with the Family Educational Rights and Privacy Act (“FERPA”), the Children’s Online Privacy Protection Act (“COPPA”) and other applicable laws.
- (2) Personal Data is hosted in Google Cloud data centers located in the United States that maintain their own rigorous industry standard certifications and compliance offerings.
- (3) Screencastify will comply with its privacy policy at <https://www.screencastify.com/privacy/policy>.
- (4) Screencastify provides regular privacy and security awareness training, including training on applicable laws that govern the handling of Personal Data, to its employees who will have access to Personal Data.
- (5) Screencastify has access control policies to limit internal access to education records and Personal Data to those individuals that are determined to have legitimate interests in order to fulfill his or her responsibilities in performing services to the Customer;
- (6) Screencastify uses encryption technology and other suitable means to protect the Personal Data in Screencastify’s custody, whether in motion or at rest, from unauthorized disclosure using industry standard or better technologies and methodologies