

## Data Processing Agreement

Posted: September 24, 2021

Prior Version: [May 5, 2021](#)

This Data Processing Agreement (the “DPA”) supplements the applicable services agreement (“Agreement”) between HelloSign and the customer that has executed or agreed to the Agreement (“Customer”). Capitalized terms used, but not defined, in this DPA are defined in the Agreement.

1. Nature of the Data and Role of the Parties. The rights and obligations in this DPA apply solely to the Processing of Personal Data by the HelloSign Service on behalf of Customer, but does not apply to Beta Releases. For the purposes of this DPA, references to Customer Data shall mean any Personal Data incorporated in the Customer Data. Customer acknowledges that the HelloSign Service is provided by technology and infrastructure maintained by HelloSign’s affiliates, Dropbox US and Dropbox International.
2. Data Processing.
  - 2.1. Instructions. The Agreement and this DPA constitute Customer’s instructions to HelloSign to Process Customer Data. HelloSign will use and Process Customer Data as Customer instructs in order to deliver the HelloSign Service and to fulfill HelloSign’s obligations under the Agreement and this DPA. HelloSign will inform Customer of any legal requirement which prevents it from complying with Customer’s instructions, unless prohibited from doing so by applicable law or on important grounds of public interest.
  - 2.2. Processing Activities. HelloSign, HelloSign personnel, and Sub-processors will only Process Customer Data to provide the HelloSign Service and to fulfill HelloSign’s obligations in this Agreement. The categories of Personal Data to be processed by HelloSign and the Processing activities to be performed under this Agreement are set out in Exhibit A.
  - 2.3. Personnel. Any HelloSign personnel who have access to Customer Data will be bound by appropriate confidentiality obligations.
3. Security.
  - 3.1. Security Measures. HelloSign will implement the technical and organizational measures set forth in the Agreement for the applicable HelloSign Service.
  - 3.2. Security Incidents. HelloSign will promptly, and without undue delay, notify Customer in writing at the email address associated with the account if a Security Incident occurs, so long as applicable law allows this notice. Without limiting the foregoing, HelloSign will use commercially reasonable efforts to provide this notice within 72 hours of confirming the existence of a Security Incident. HelloSign may limit the scope of, or refrain from delivering, any disclosures to the extent reasonably necessary to avoid compromising the integrity of HelloSign’s security, an ongoing investigation, or any HelloSign customer’s or end user’s data.
  - 3.3. Notification. HelloSign will assist the Customer in ensuring compliance with its obligations pursuant to EU Data Protection Laws by providing relevant information which may include: (a) the nature of the Security Incident, including, where possible, the categories and approximate number of personal data records concerned; (b) the likely consequences of the Security Incident; (c) the measures taken or to be taken to address the Security Incident, including, where appropriate, the measures to mitigate its possible adverse effects; (d) the name and contact details of the Data Protection Officer or other contact from whom more information may be obtained; and (e) justifications for any delay in notification;. Should it not be feasible for HelloSign to provide all of the relevant information in its initial notification to the Customer, HelloSign will provide further relevant details without undue delay.
4. Sub-processors.
  - 4.1. HelloSign Use of Sub-Processors. Customer consents to HelloSign’s appointment of Subcontractors, including Sub-processors, to perform the HelloSign Service. Where a Sub-processor will process Personal Data, HelloSign will ensure that the Sub-processor is subject to substantially similar data protection obligations as those set forth in this DPA regarding Personal Data and which satisfy the requirements of EU Data Protection Laws. HelloSign will list its current Sub-processors for the HelloSign Service at <https://hellosign.com/subprocessors>. HelloSign will remain liable for all acts or omissions of its Subcontractors or Sub-processors, and for any subcontracted obligations.
  - 4.2. Customer Objections. HelloSign may add or remove Sub-processors from time to time. HelloSign will inform Customer in advance of new Sub-processors for the applicable HelloSign Service as described in the list of Sub-processors. If Customer objects to a change, it will provide HelloSign with notice of its objection to [privacy@dropbox.com](mailto:privacy@dropbox.com) including reasonable detail supporting Customer’s concerns within sixty days of

receiving notice of a change from HelloSign or, if Customer has not subscribed to receive this notice, within sixty days of HelloSign publishing the change. HelloSign will then use commercially reasonable efforts to review and respond to Customer's objection within thirty days of receipt of Customer's objection. HelloSign's response to Customer's objection will include, at a minimum, reasonable accommodations, if any, that Customer or HelloSign can take to limit or prevent a new Sub-processor from acting as a processor of Customer Data when Customer makes use of the HelloSign Service. If HelloSign does not respond to a Customer objection as described above, or cannot reasonably accommodate Customer's objection, Customer may terminate the Agreement by providing written notice to HelloSign: (a) within thirty days of receipt of a HelloSign response that does not comply with this Section 4.2; or (b) if HelloSign fails to respond, within thirty days of the date HelloSign's response was due.

5. Data Subject Rights. Customer is responsible for responding to any request by a data subject to exercise their rights under applicable privacy laws. If HelloSign receives any such request in relation to the Customer Data, HelloSign will direct the applicable data subject to Customer to exercise his or her rights without undue delay after verifying the request pertains to Customer Data. HelloSign will provide Customer with information or tools that are reasonably designed to enable Customer to fulfill its obligations to respond to these requests through the functionality of the HelloSign Service, taking into account the nature of the Processing and insofar as this is possible.
6. Compliance Assistance. To assist Customer with its compliance obligations under applicable privacy laws related to security, data protection impact assessments, and prior consultation with supervisory authorities, HelloSign will make the following available during the Term: (a) the Audit Reports; (b) the information contained in Exhibit A; and (c) any applicable Security Measures and Security Resources set forth in the Agreement. If, after reviewing the aforementioned materials, Customer reasonably believes it needs further information in order to meet its compliance obligations, HelloSign will use commercially reasonable efforts to respond to written questions by Customer regarding the materials. Without limiting the foregoing, HelloSign will comply with valid requests from relevant supervisory authorities to the extent required by applicable EU Data Protection Law.
7. Deletion. Upon Termination of the Agreement and this DPA, HelloSign will delete Customer Data in Customer's account in a commercially reasonable period of time following receipt of Customer's request to do so prior to such termination. Notwithstanding the foregoing, Customer acknowledges and agrees that HelloSign may be a controller with respect to certain account data, and may retain this data in accordance with applicable privacy laws, provided that HelloSign is solely responsible for its compliance with these laws in connection with its own Processing.
8. Inspections.
  - 8.1. Audit Reports. HelloSign has completed audits for the HelloSign Service as set forth in the Agreement and will provide Customer with a copy of the Audit Reports as set forth therein.
  - 8.2. Customer Review of Audit Reports. If Customer reasonably believes it needs further information in order to confirm HelloSign's compliance with the provisions of the Agreement relating to Personal Data, HelloSign will use commercially reasonable efforts to respond to written questions by Customer regarding the Audit Reports.
  - 8.3. Customer Inspection. If Customer is not satisfied with HelloSign's responses to questions provided pursuant to Section 8.2, HelloSign will permit Customer, or an agreed upon Customer representative, subject to appropriate confidentiality obligations, to visit HelloSign's premises and discuss HelloSign's responses with HelloSign personnel.
  - 8.4. Process for Inspections. HelloSign reserves the right to: (a) charge a separate fee for its reasonable costs associated with performing any of its obligations in Section 8.2 or 8.3, provided that HelloSign will provide an estimate of these fees to Customer prior to incurring the costs; or (b) object to any Customer representative participating in an inspection on the basis that they are not qualified, are not bound by an adequate requirement to protect confidential HelloSign information, or are a competitor of HelloSign. For Customer inspections pursuant to Section 8.3, the Parties will first mutually agree on the scope, timing, and duration of the inspection. HelloSign reserves the right to limit the scope and duration of an inspection to the extent reasonably necessary to avoid compromising the integrity of HelloSign's security or any HelloSign customer's or end user's data.
9. European Data. Customer agrees that HelloSign and its Sub-processors may transfer, store, and Process Customer Data in locations other than Customer's country. To the extent European Data is Processed outside of the EEA, United Kingdom, or Switzerland, this Section 9 applies.
  - 9.1. Instructions. Customer hereby instructs Dropbox International to process European Data in accordance with this DPA in order to deliver the HelloSign Service. Customer acknowledges that all communication with HelloSign in

connection with the processing of European Data will be coordinated and directed through Dropbox International.

- 9.2. Transfers. Customer acknowledges and agrees that, to provide the HelloSign Service, Dropbox International may transfer European Data to Dropbox US and this transfer will be made pursuant to the Processor to Processor Standard Contractual Clauses between HelloSign and Dropbox International, or an alternative transfer means recognized by EU Data Protection Laws.
10. Insurance. HelloSign maintains reasonable coverage for Technology Errors and Omissions insurance, which may include coverage for privacy and network security liability, losses or damages due to the unauthorized use/access of a computer system or database, and defense of any regulatory action involving a breach of privacy, as well as other coverage areas. Upon Customer's reasonable written request, and no more than once per year, HelloSign will provide a certificate of insurance evidencing its coverages.
11. Effect of DPA. If a provision in this DPA conflicts with a provision in the Agreement, then this DPA will control with respect to the processing of Personal Data. The Agreement will remain in full force and effect and will be unchanged except as modified by this DPA. This DPA will terminate automatically upon expiration or termination of the Agreement.
12. Definitions.
- "Dropbox International" means Dropbox International Unlimited Company.
- "Dropbox US" means Dropbox, Inc.
- "EU Data Protection Laws" means, to the extent in force and applicable from time to time, those laws implementing the EU General Data Protection Regulation (2016/679) and any implementing laws in each EU member state.
- "European Data" means Personal Data that is subject to EU Data Protection Laws.
- "Personal Data," "Process," and "Processing" have the meaning given to those terms in the EU Data Protection Laws.
- "Security Incident" means any actual unauthorized disclosure of or access to Customer Data, or compromise of HelloSign's systems that HelloSign determines is reasonably likely to result in such disclosure or access, caused by failure of HelloSign's Security Measures and excluding any unauthorized disclosure or access that is caused by Customer or its end users, including Customer or its end users' failure to adequately secure equipment or accounts.
- "Security Measures" means the technical and organizational security measures implemented for the HelloSign Service, as may be further described in the Agreement.
- "Subcontractor" means an entity to whom HelloSign subcontracts any of its obligations under the Agreement.
- "Sub-processor" means an entity who agrees to Process Customer Data on HelloSign's behalf, or on behalf of another Dropbox sub-processor, in order to deliver the HelloSign Service.

## Exhibit A

### Details of Processing.

1. Subject Matter of the Personal Data Processing: The provision of the HelloSign Service by HelloSign to Customer.
2. Duration of the Personal Data Processing: The Term, and any period after the Term prior to HelloSign's deletion of Customer Data.
3. Nature and Purpose of the Personal Data Processing: To enable Customer to receive and HelloSign to provide the HelloSign Service.
4. Categories of Personal Data: The Personal Data that will be included in Customer Data will depend upon Customer's use of the Services. To the extent the Customer Data contains Personal Data, it may consist of identifying information of end users (such as name, email address, physical address, IP address, or other unique identifier), identifying information of third parties with whom data is shared or to whom signature requests are sent, organization data, and any other Personal Data contained in documents, images and other content or data in electronic form stored or transmitted by End Users via the HelloSign Service.
5. Data Subjects: The categories of data subjects will depend upon Customer's use of the Services. To the extent the Customer Data contains Personal Data, it may concern Customer's End Users including employees, contractors, collaborators and customers of the Customer, any individuals collaborating, sharing, or transacting with these End Users, or any other individual whose information is stored by Customer in the Customer Data as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR.