

Data Processing Agreement

Posted: May 5, 2021

This Data Processing Agreement (the “DPA”) supplements the applicable terms (either the HelloSign Terms of Use / Service or the Master Services Agreement) between JN Projects, Inc. d/b/a HelloSign (“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 regarding data subjects in the EEA (“EU Personal Data”) by the Services by HelloSign on behalf of Customer, but does not apply to Beta Services. For the purposes of this DPA, references to Customer Data shall mean any EU Personal Data incorporated in the Customer Data.
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 Services 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 and its Sub-processors will only Process Customer Data to provide the Services 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 appropriate technical and organisational security measures designed to protect Personal Data against: **(i)** unauthorised or unlawful processing; **(ii)** accidental or unlawful destruction; **(iii)** accidental loss or alteration; and **(iv)** unauthorised disclosure or access. HelloSign’s current measures are specified at <https://www.hellosign.com/trust/security> (the “**Security Standards**”). Customer has reviewed the Security Standards and agrees that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the Personal Data to be protected. HelloSign has no responsibility for the security, availability or integrity of Customer’s own systems or Third Party Products integrated with the HelloSign Service. Customer agrees that it is solely responsible for its own use of the HelloSign Service, including securing its account authentication credentials and choosing appropriate privacy and security settings for the HelloSign Service.
 - 3.2. Security Incidents. HelloSign will promptly, and without undue delay, notify Customer if a Security Incident occurs, so long as applicable law allows this notice. 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. “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 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.
4. Sub-processors.
 - 4.1. HelloSign Use of Sub-Processors. Customer consents to HelloSign’s appointment of Subcontractors, including Sub-processors, to perform the Services. Where a Sub-processor will process EU Personal Data, HelloSign will ensure that the Sub-processor is subject to contractual obligations regarding EU Personal Data which satisfy the requirements of EU Data Protection Laws. HelloSign will list its current Sub-processors at <https://hellosign.com/subprocessors> or another link provided by HelloSign from time to time. 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 of new Sub-processors. If Customer objects to a change, it will provide HelloSign with notice of its objection to privacy@dropbox.com including reasonable detail supporting Customer’s concerns within thirty 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 Services. 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 EU Data Protection 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 under EU Data Protection Laws 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 Services, taking into account the nature of the Processing and insofar as this is possible.
6. Deletion. Upon Termination of the Agreement and this DPA, HelloSign will delete Personal Data in Customer's account in a commercially reasonable period of time following receipt of a 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 EU Data Protection Laws, provided that HelloSign is solely responsible for its compliance with these laws in connection with its own Processing.
7. Audits and Inspections.
 - 7.1. By Supervisory Authorities. HelloSign will provide Customer with reasonable access to its documentation and systems in the event of an audit required by a government regulator or supervisory authority for compliance with EU Data Protection Laws.
 - 7.2. By Customers. Customer may request that HelloSign make available documentation reasonably necessary to demonstrate compliance with the obligations under GDPR Article 28, including the executive summary of HelloSign's annual security audit conducted by an independent, third party auditor. Except with respect to audits required by a government regulator or supervisory authority, Customer agrees to exercise its audit rights under applicable EU Data Protection Laws by requesting the above information. Without limiting Customer's responsibilities under this DPA, HelloSign will use reasonable efforts to inform Customer if it discovers, in connection with an audit described in GDPR Article 28(3)(h), information that in HelloSign's opinion would cause Customer's Instructions to infringe EU Data Protection Laws. Any requests under this Section may occur no more than once per calendar year.
 - 7.3. Other Provisions. The parties will mutually agree on the timing and scope of any audits, which will be: (i) carried out in such a way as to not disrupt HelloSign's business; (ii) performed at Customer's sole expense, including reimbursement for HelloSign's time spent on any on-site inspections; and (iii) subject to reasonable confidentiality protections requested by HelloSign. Any executive summaries, audit reports or other information obtained by Customer will be considered HelloSign's Confidential information. HelloSign will not be required to disclose any commercial secrets, including algorithms, source code, trade secrets and similar information.
8. Transfers. 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 EU Personal Data is Processed outside of the EEA, this Section 9 applies.
 - 8.1. Privacy Shield. HelloSign is certified and complies with the EU-U.S. Privacy Shield Program with respect to the collection, use and retention of EU Personal Data transferred from the EEA to the United States. If the Privacy Shield Program is invalidated, HelloSign will use commercially reasonable efforts to comply with alternate or successor data transfer mechanisms.
 - 8.2. Model Clauses. If EU Personal Data is transferred from the EEA to: (a) any country other than the United States that has not been found to provide adequate safeguards; or (b) the United States if the Privacy Shield Program is invalidated and no alternate or successor data transfer mechanism exists or HelloSign is unable to comply with the new mechanism, the terms of the transfer shall be governed by the EU Standard Contractual Clauses attached hereto as Exhibit B.
9. 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 EU Personal Data. The Agreement will remain in full force and effect and will be unchanged except as modified by this DPA. This DPA and the EU Standard Contractual Clauses will terminate automatically upon expiration or termination of the Agreement.

Exhibit A

Details of Processing.

1. Subject Matter of the Personal Data Processing: The provision of the Services 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 Services.
4. Categories of Personal Data:
 - *Customer Account Data*: Name, email address, password, contact details, and similar personal data provided when creating an account.
 - *Signatory / Transactional Data*: Name, email address, contact details, and similar personal data provided when a signature is requested from an individual or transaction involves an individual.
5. Data Subjects: To the extent the Customer Data contains Personal Data, it may concern Customer's End Users, any individuals collaborating or sharing with these End Users, or any other individual whose information is stored by Customer.

Exhibit B

Commission Decision C(2010)593

EU Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization: The Customer that is a party to the HelloSign Terms of Use or the HelloSign Enterprise Agreement

(the "Data Exporter")

And

Name of the data importing organization: JN Projects, Inc.

Address: 1800 Owens Street, Suite 200, San Francisco, CA 94107 USA

(the "Data Importer")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses), in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

- a. "personal data," "special categories of data," "process/processing," "controller," "processor," "Data Subject" and "supervisory authority" shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- b. "the Data Exporter" means the controller who transfers the personal data;
- c. "the Data Importer" means the processor who agrees to receive from the Data Exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- d. "the Sub-Processor" means any processor engaged by the Data Importer or by any other Sub-Processor of the Data Importer who agrees to receive from the Data Importer or from any other Sub-Processor of the Data Importer personal data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- e. "the applicable data protection law" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the Data Exporter is established;
- f. "technical and organizational security measures" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The Data Subject can enforce against the Data Exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The Data Subject can enforce against the Data Importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the Data Exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the Data Exporter, in which case the Data Subject can enforce them against such entity.
3. The Data Subject can enforce against the Sub-Processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the Data Exporter, in which case the Data Subject can enforce them against such entity. Such third-party liability of the Sub-Processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a Data Subject being represented by an association or other body if the Data Subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the Data Exporter

The Data Exporter agrees and warrants:

- a. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the Data Exporter is established) and does not violate the relevant provisions of that State;
- b. that it has instructed and throughout the duration of the personal data-processing services will instruct the Data Importer to process the personal data transferred only on the Data Exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- c. that the Data Importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;
- d. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- e. that it will ensure compliance with the security measures;
- f. that, if the transfer involves special categories of data, the Data Subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- g. to forward any notification received from the Data Importer or any Sub-Processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the Data Exporter decides to continue the transfer or to lift the suspension;
- h. to make available to the Data Subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for Sub-Processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- i. that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a Sub-Processor providing at least the same level of protection for the personal data and the rights of Data Subject as the Data Importer under the Clauses; and
- j. that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the Data Importer

The Data Importer agrees and warrants:

- a. to process the personal data only on behalf of the Data Exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Exporter of its inability to comply, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;
- b. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Data Exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the Data Exporter as soon as it is aware, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;
- c. that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;
- d. that it will promptly notify the Data Exporter about:
 - i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
 - ii. any accidental or unauthorized access; and
 - iii. any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorized to do so;
- e. to deal promptly and properly with all inquiries from the Data Exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- f. at the request of the Data Exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the Data Exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Data Exporter, where applicable, in agreement with the supervisory authority;
- g. to make available to the Data Subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the Data Subject is unable to obtain a copy from the Data Exporter;
- h. that, in the event of sub-processing, it has previously informed the Data Exporter and obtained its prior written consent;
- i. that the processing services by the Sub-Processor will be carried out in accordance with Clause 11;
- j. to send promptly a copy of any Sub-Processor agreement it concludes under the Clauses to the Data Exporter.

Clause 6

Liability

1. The parties agree that any Data Subject, who has suffered damage as a result of any breach of the obligations, referred to in Clause 3 or in Clause 11 by any party or Sub-Processor is entitled to receive compensation from the Data Exporter for the damage suffered.
2. If a Data Subject is not able to bring a claim for compensation in accordance with paragraph 1 against the Data Exporter, arising out of a breach by the Data Importer or his Sub-Processor of any of their obligations referred to in Clause 3 or in Clause 11, because the Data Exporter has factually disappeared or ceased to exist in law or has become insolvent, the Data Importer agrees that the Data Subject may issue a claim against the Data Importer as if it were the Data Exporter, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. The Data Importer may not rely on a breach by a Sub-Processor of its obligations in order to avoid its own liabilities.
3. If a Data Subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in paragraphs 1 and 2, arising out of a breach by the Sub-Processor of any of their obligations referred to in Clause

3 or in Clause 11 because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, the Sub-Processor agrees that the Data Subject may issue a claim against the data Sub-Processor with regard to its own processing operations under the Clauses as if it were the Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. The liability of the Sub-Processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The Data Importer agrees that if the Data Subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the Data Importer will accept the decision of the Data Subject:
 - a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - b. to refer the dispute to the courts in the Member State in which the Data Exporter is established.
2. The parties agree that the choice made by the Data Subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The Data Exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the Data Importer, and of any Sub-Processor, which has the same scope and is subject to the same conditions as would apply to an audit of the Data Exporter under the applicable data protection law.
3. The Data Importer shall promptly inform the Data Exporter about the existence of legislation applicable to it or any Sub-Processor preventing the conduct of an audit of the Data Importer, or any Sub-Processor, pursuant to paragraph 2. In such a case the Data Exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the Data Exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the Sub-Processor which imposes the same obligations on the Sub-Processor as are imposed on the Data Importer under the Clauses. Where the Sub-Processor fails to fulfill its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the Sub-Processor's obligations under such agreement.
2. The prior written contract between the Data Importer and the Sub-Processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the Data Subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the Data Exporter or the Data Importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law. Such third-party liability of the Sub-Processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the Data Exporter is established.
4. The Data Exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by

the Data Importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Data Exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the Data Importer and the Sub-Processor shall, at the choice of the Data Exporter, return all the personal data transferred and the copies thereof to the Data Exporter or shall destroy all the personal data and certify to the Data Exporter that it has done so, unless legislation imposed upon the Data Importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the Data Importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The Data Importer and the Sub-Processor warrant that upon request of the Data Exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Additional Provisions

Capitalized terms used in Sections A to D and the Appendices but not defined in the Clauses are defined in the Agreement.

- A. Security Audit. The data importer maintains ISO/IEC 27001 and ISO/IEC 27018 certifications, which are issued by an independent third party auditor. The data importer will continue to undergo regular ISO/IEC 27001:2013 and ISO/IEC 27018 audits necessary for maintaining such certifications for the Services during the Term. The data importer also regularly undergoes Service Organization Control 2 (SOC 2) Type II audits. Subject to the data importer's confidentiality obligations and no more than once a year, the data importer will provide the data exporter with a copy of the SOC 2 Type II Report upon written request. The data importer will make new SOC 2 reports available as they are completed subject to the data importer's confidentiality requirements.

The data exporter agrees that the data importer's obligations set forth in this Section A and Section 8 of this DPA fully satisfy the audit rights under Clause 5(f) and Clause 12 (2) of the Clauses.

- B. Sub-processing. The data importer may engage other companies to provide limited parts of the Services (including support services) on the data importer's behalf, and the data exporter consents to the data importer subcontracting the processing of personal data to such sub-processors as described in the Clauses. The data importer will ensure that any sub-processor will only access and use personal data to provide the Services as set forth in a written agreement between the data importer and the sub-processor. The data exporter acknowledges that any requirements applicable to the data importer under the Clauses in respect of agreements with sub-processors shall be satisfied in full provided that the sub-processing agreement between the data importer and the sub-processor provides at least the level of data protection required under the HelloSign Terms.
- C. Liability. The Clauses shall be subject to the limitations and exclusions of liability contained in the "Limitation of Liability" section of the HelloSign Terms, such that the total liability of the data importer and HelloSign, in aggregate, shall not exceed the limitations set out in the HelloSign Terms.
- D. Application. This DPA and the EU Standard Contractual Clauses apply to data processed by the Services as this term is defined in the Agreement, and future variations of the Services, but does not apply to BetaServices.

Appendix 1 to the EU Standard Contractual Clauses

This Appendix forms part of the Clauses.

Data Exporter

The Data Exporter is the customer to the Agreement, as amended by the DPA.

Data Importer

The Data Importer is JN Projects, Inc. d/b/a/ HelloSign (“HelloSign”), a global provider of cloud services for individuals and business. HelloSign provides a website, software and mobile applications that allow people to streamline complex transactions through innovative digital solutions such as electronic fax, electronic signature, and workflow automation. HelloSign’s service may also be accessed by Application Programming Interfaces (APIs).

Data Subjects

The personal data transferred concern the Data Exporter’s and Data Exporter’s affiliates’ end users including employees, consultants and contractors of the Data Exporter, any individuals collaborating or sharing with these end users using the services provided by Data Importer, or any other individual whose information is stored by Customer.

Categories of data

The personal data transferred concern end users identifying information and organization data (both on-line and off-line) as well as documents, images and other content or data in electronic form stored or transmitted by end users via Data Importer’s services.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Scope of Processing.

The scope and purposes of processing the Data Exporter’s personal data is described in the DPA to which these Clauses are annexed as well as the Agreement between Data Exporter and Data Importer.

Term of Processing.

The term for data processing will be the term set forth in the applicable Agreement.

Data Deletion or Return.

Upon expiration or termination of the Agreement, Data Importer agrees to delete or return Data Exporter’s personal data from Data Importer’s service, in accordance with the terms and conditions of the Agreement.

Access to Data.

Data Exporter may designate an administrator who will have the ability to access Data Exporter’s personal data in accordance with the Agreement. In addition, an individual end user of Data Exporter will have the ability to access any of such end user’s personal data associated with the specific account through which such end user accesses and uses the service in accordance with the functionality of the service, the Agreement and the agreement between HelloSign and the individual Data Exporter end user.

Sub-processing.

Data Importer may engage other companies to provide parts of the service on Data Importer’s behalf. Data Importer will ensure that any such Sub-Processors will only access and use any personal data of Data Exporter to provide the service in accordance with the Agreement.

Appendix 2 to the EU Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data Privacy Contact

The data privacy officer of the Data Importer can be reached at privacy@dropbox.com.

Security Measures

Data Importer has implemented the Security Measures set forth in the Data Processing Agreement entered into by Data Importer and Data Exporter.