

DATA PROTECTION ATTACHMENT FOR DOCUSIGN SERVICES

If you started your subscription before December 1, 2022, please go here: (<https://www.docusign.com/legal/agreements/legacy/>) to review your terms.

Version Date: December 1, 2022

This Data Protection Addendum for DocuSign Services (“**DPA**”) is incorporated into and made part of the Agreement. Unless otherwise defined in this DPA, capitalized terms will have the meaning given to them in the Agreement. In the event of any conflict between these documents, the following order of precedence applies (in descending order): (a) Binding Corporate Rules; (b) the Standard Contractual Clauses as provided in herein; (c) the body of the DPA; (d) any documents attached to the DPA; and (e) the Agreement.

1. DEFINITIONS. For purposes of this DPA:

“**Binding Corporate Rules**” means DocuSign’s Binding Corporate Rules for Processors, the most current version of which is available on DocuSign’s website at <https://trust.docusign.com/en-us/trust-certifications/gdpr/bcr-p-processor-privacy-code/>.

“**Controller,**” “**Business,**” “**Processor,**” and “**Service Provider**” (or equivalent terms) have the meanings set forth under Data Protection Laws.

“**Data Breach**” means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data managed by DocuSign.

“**Data Protection Laws**” means all applicable laws, regulations, and other legally binding requirements in any jurisdiction relating to privacy, data protection, data security, breach notification, that apply to DocuSign’s Processing of Personal Data, including, without limitation, to the extent applicable, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* and any associated regulations and amendments, including, when effective, the California Privacy Rights Act amendments (“**CCPA**”); the General Data Protection Regulation, Regulation (EU) 2016/679 (“**GDPR**”); the Swiss Federal Act on Data Protection (“**FADP**”); the United Kingdom Data Protection Act of 2018 (“**UK GDPR**”); the Australian Privacy Act (No. 119, 1988) (as amended) (“**the Privacy Act**”); the Canadian Personal Information Protection and Electronic Documents Act

(“**PIPEDA**”); Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019) (“**LGPD**”); and the Singapore Personal Data Protection Act 2012 (No. 26 of 2012) (“**PDPA**”).

“**Data Subject**” means an identified or identifiable natural person about whom Personal Data relates (or equivalent term under Data Protection Laws).

“**EU SCCs**” means the Standard Contractual Clauses issued pursuant to 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*, located http://data.europa.eu/eli/dec_impl/2021/914/oj, and completed as set forth in Section 7 below.

“**Personal Data**” includes “personal data,” “personal information,” “personally identifiable information,” or equivalent terms that is Processed by DocuSign in connection with providing DocuSign Services under the Agreement, and such terms shall have the same meaning as defined by Data Protection Laws.

“**Process**” and “**Processing**” has the meaning set forth under Data Protection Laws and the Security Attachment for DocuSign Services, and includes any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

2. SCOPE AND PURPOSES OF PROCESSING.

2.1 Depending on Data Protection Laws, Customer is a Controller or Business and DocuSign is a Processor or Service Provider with respect to DocuSign’s Processing of Personal Data to provide the DocuSign Services under the Agreement. This DPA applies to DocuSign’s Processing of Personal Data on Customer’s or Customer Affiliate’s behalf (as applicable) for the provision of the DocuSign Services as specified in the Agreement.

2.2 The scope, nature, purposes, and duration of the processing, the types of Personal Data Processed, and the Data Subjects concerned are set forth in this DPA, including its Schedule A. The details provided in Schedule A are deemed to satisfy any requirement to provide such details under any Data Protection Laws.

2.3 DocuSign will Process Personal Data solely: (a) to fulfill its obligations to Customer under the Agreement, including this DPA; (b) on Customer’s behalf pursuant to Customer’s instructions; and (c) in compliance with Data Protection Laws. DocuSign will not “sell” Personal Data

(as such term in quotation marks is defined in Data Protection Laws), “share” or Process Personal Data for purposes of “cross-context behavioral advertising” or “targeted advertising” (as such terms are defined in Data Protection Laws), or otherwise Process Personal Data for any purpose other than for the specific purposes set forth herein or outside of the direct business relationship with Customer. DocuSign will not attempt to link, identify, or otherwise create a relationship between Personal Data and non-personal data or any other data without the express authorization of Customer.

2.4 Customer will ensure that: (a) all such notices have been given, and all such authorizations have been obtained, as required under Data Protection Laws, for DocuSign (and its Affiliates and Subprocessors) to process Personal Data as contemplated by the Agreement and this DPA; (b) it has complied, and will continue to comply, with all Data Protection Laws; and (c) it has, and will continue to have, the right to transfer, or provide access to, Personal Data to DocuSign for Processing in accordance with the terms of the Agreement and this DPA.

2.5 Unless otherwise specified in the Agreement, Customer agrees it will not provide DocuSign with any sensitive or special categories of Personal Data that impose specific data security or data protection obligations on DocuSign in addition to or different from those specified in this DPA (including any appendix to the DPA) or Agreement.

3. PERSONAL DATA PROCESSING REQUIREMENTS. DocuSign will:

(a) Ensure that the persons it authorizes to Process the Personal Data are subject to confidentiality obligations regarding such activity or are under an appropriate statutory obligation of confidentiality.

(b) Promptly notify Customer of: (i) any third-party or Data Subject complaints regarding the Processing of Personal Data; or (ii) any government request for access to or information about DocuSign’s Processing of Personal Data on Customer’s behalf, unless prohibited by applicable laws. DocuSign will provide Customer with commercially reasonable cooperation and assistance in relation to any such request. If DocuSign is prohibited by applicable laws from disclosing the details of a government request to Customer, DocuSign shall use all available legal mechanisms to challenge any demands for data access through the applicable government process that it receives, as well as any non-disclosure provisions attached thereto as set forth in DocuSign’s Law Enforcement Guidelines, available at <https://www.docusign.com/legal/law-enforcement>.

(c) Provide reasonable assistance to and cooperation with Customer for Customer’s performance of a data protection impact assessment of Processing or proposed Processing of Personal Data, when required by Data Protection Laws.

(d) Provide commercially reasonable assistance to and cooperation with Customer for Customer’s consultation with regulatory authorities in relation to the Processing or proposed Processing of Personal Data, including complying with any obligation applicable to DocuSign under Data

Protection Laws to consult with a regulatory authority in relation to DocuSign's Processing or proposed Processing of Personal Data.

(e) Comply with the CCPA's restrictions pursuant to 1798.140 (e)(6) regarding combining Personal Data with personal data received from, or on behalf of, another person or persons for the purposes enumerated in the CCPA. With respect to its obligations under CCPA, DocuSign certifies that it will comply with them under this DPA (including, without limitation to, the restrictions under Sections 2 and 3).

(f) Promptly notify Customer if it determines that: (i) it can no longer meet its obligations under this DPA or Data Protection Laws; or (ii) in its opinion, an instruction from Customer infringes Data Protection Laws.

4. DATA SUBJECT REQUESTS.

4.1 If DocuSign receives a direct request from a Data Subject regarding rights under Data Protection Laws, DocuSign will promptly notify the request to Customer if the Data Subject has identified Customer as Controller of the Personal Data subject to the request and may inform the Data Subject that it has done so. DocuSign will provide reasonable assistance to Customer in fulfilling its obligations under Data Protection Laws to respond to Data Subject requests, but Customer understands and agrees that, as a Controller, Customer is solely responsible for responding to such Data Subject's requests or inquiries and that DocuSign has no responsibility to respond to a Data Subject for or on behalf of Customer.

4.2 If Customer receives a request or inquiry from a Data Subject related to Personal Data Processed by DocuSign, Customer can either: (a) access its DocuSign Services containing Personal Data to address the request or inquiry; or (b) to the extent such access is not available to Customer, contact DocuSign customer support for additional assistance to enable Customer to address the request or inquiry.

5. DATA SECURITY.

5.1 DocuSign will implement appropriate administrative, technical, physical, and organizational measures to protect Personal Data. Details regarding the specific security measures that apply to the DocuSign Services are as described in the Binding Corporate Rules, the Agreement and in the Security Attachment for DocuSign Services. Customer acknowledges that DocuSign's security measures are subject to technical progress and development and that DocuSign may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the DocuSign Services purchased by Customer.

5.2 Customer shall be responsible for properly implementing access and use controls and configuring certain features and functionalities of the DocuSign Services that Customer may elect to use and agrees that it will do so in accordance with this DPA and the Agreement in such manner

that Customer deems adequate, including, without limitation, maintaining appropriate security, protection, deletion, and backup of its own Personal Data.

6. DATA BREACH. DocuSign will notify Customer without undue delay upon becoming aware of any Data Breach and will assist Customer in Customer's compliance with its Data Breach-related obligations, including, without limitation, by:

(a) Taking commercially reasonable steps to mitigate the effects of the Data Breach and reduce the risk to Data Subjects whose Personal Data was involved; and

(b) Providing Customer with the following information, to the extent known:

(i) The nature of the Data Breach, including, where possible, how the Data Breach occurred, the potential categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;

(ii) The likely consequences of the Data Breach; and

(iii) Measures taken or proposed to be taken by DocuSign to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects and causes.

(c) DocuSign's obligation to report a Data Breach under this DPA is not and will not be construed as an acknowledgement by DocuSign of any fault or liability of DocuSign with respect to such Data Breach. Customer is solely responsible for determining whether to notify impacted Data Subjects and for providing such notice, and for determining whether relevant supervisory authorities need to be notified of a Data Breach as may be required for Customer's own business and activities. Notwithstanding the foregoing, Customer agrees to reasonably coordinate with DocuSign on the content of Customer's intended public statements or required notices for affected Data Subjects and/or notices to relevant supervisory authorities regarding the Data Breach.

7. SUBPROCESSORS.

7.1 Customer acknowledges and agrees that DocuSign may use DocuSign Affiliates and other Subprocessors (as defined in Data Protection Law) to Process Personal Data in accordance with the provisions within this DPA and Data Protection Laws. Where DocuSign subcontracts any of its rights or obligations concerning Personal Data, including to any Affiliate, DocuSign will take steps to select and retain Subprocessors that are capable of maintaining appropriate privacy and security measures to protect Personal Data consistent with Data Protection Laws and this

DPA and will remain liable for the performance of all its obligations under the Agreement and this DPA, whether or not performed by DocuSign, its Affiliates or Subprocessors.

7.2 DocuSign's Services Subprocessor List is available on DocuSign's website at <https://www.docusign.com/trust/privacy/subprocessors-list> (the "**Subprocessor List**"), and notice regarding new DocuSign Service Subprocessors is made available through a subscription mechanism as described on the DocuSign website. Customer agrees to subscribe to the Subprocessor List for DocuSign to notify Customer of new Subprocessor(s) for the applicable DocuSign Services. DocuSign will maintain an up-to-date list of its Subprocessors, and it will provide Customer with thirty (30) days' prior notice of any new Subprocessor added to the list. In the event Customer has a commercially reasonable objection to a new Subprocessor, DocuSign will use reasonable efforts to make available to Customer a change in the DocuSign Services or recommend a commercially reasonable change to Customer's use of the DocuSign Services to avoid Processing of Personal Data by the objected-to Subprocessor without a material change to Customer's use of the affected DocuSign Services. Customer may, in its sole discretion, terminate the Agreement in the event that DocuSign is not able to provide a reasonable change to cure Customer's Subprocessor objection.

8. INTERNATIONAL DATA TRANSFERS.

8.1 DocuSign will not engage in any cross-border Processing of Personal Data, or transmit, directly or indirectly, any Personal Data to any country outside of the country from which such Personal Data was collected, without complying with Data Protection Laws. Where DocuSign engages in an onward transfer of Personal Data, DocuSign shall ensure that a lawful data transfer mechanism is in place prior to transferring Personal Data from one country to another.

8.2 To the extent DocuSign's cross-border Processing of Personal Data involves a transfer of Personal Data subject to cross-border transfer obligations under Data Protection Laws, the Binding Corporate Rules apply to the Processing of Personal Data by DocuSign and/or its Affiliates as part of the provision of DocuSign Services under the Agreement. The Binding Corporate Rules are incorporated by reference into this DPA, and DocuSign agrees to use commercially reasonable efforts to maintain the regulatory authorization of the Binding Corporate Rules or other appropriate cross-border transfer safeguards for the duration of the Agreement.

8.3 Notwithstanding section 8.2 above, to the extent legally required, by signing this DPA, Customer and DocuSign are deemed to have signed the EU SCCs as an additional safeguard, which form part of this DPA and (except as described in Section 7(d) and (e) below) will be deemed completed as follows:

- (a)** Module 2 of the EU SCCs applies to transfers of Personal Data from Customer (as a Controller) to DocuSign (as a Processor) and Module 3 applies to transfers of Personal Data from Customer (as a Processor) to DocuSign (as a Subprocessor);
- (b)** Clause 7 (the optional docking clause) is included;
- (c)** Under Clause 9 (Use of Subprocessors), the Parties select Option 2 (General written authorization);
- (d)** Under Clause 11 (Redress), the optional language requiring that Data Subjects be permitted to lodge a complaint with an independent dispute resolution body shall not be deemed to be included;
- (e)** Under Clause 17 (Governing law), the Parties choose Option 1 (the law of an EU Member State that allows for third-Party beneficiary rights). The Parties select the laws of Ireland;
- (f)** Under Clause 18 (Choice of forum and jurisdiction), the Parties select the courts of Ireland;
- (g)** Annex I(A) and I(B) (List of Parties) is completed as set forth in Schedule A;
- (h)** Under Annex I(C) (Competent supervisory authority), the Parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Irish Data Protection Commission;
- (i)** Annex II (Technical and organizational measures) is completed as provided in Schedule A of this DPA; and
- (j)** Annex III (List of Subprocessors) is not applicable as the Parties have chosen General Authorization under Clause 9; however, DocuSign's Subprocessor list can be viewed as described above in Section 6.

8.4 With respect to Personal Data transferred from the United Kingdom, for which the UK GDPR (and not the GDPR or FADP) governs the international nature of the transfer, the International Data Transfer DPA to the EU SCCs (available as of the Effective Date at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>) ("**UK SCCs**") forms part of this DPA and takes precedence over the rest of this DPA as set forth in the UK SCCs. Undefined capitalized terms used in this provision shall mean the definitions in the UK SCCs. The UK SCCs shall be deemed complete as follows: (a) the Parties' details shall be the Parties and their Affiliates to the extent any of them are involved in such transfer; (b) the Key Contacts shall be the contacts set forth in the Agreement; (c) the Approved EU SCCs referenced in Table 2 shall be the EU SCCs as executed by the Parties; (d) either Party may end this DPA as set out in Section 19 of the UK SCCs; and (e) by entering into this DPA, the Parties are deemed to be signing the UK SCCs.

8.5 For transfers of Personal Data that are subject to the FADP, the EU SCCs form part of this DPA as set forth in Section 8.3 of this DPA, but with the following differences, to the extent required by the FADP: (a) references to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR; (b) references to personal data in the EU SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope; (c) the term “Member State” in EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs; and (d) the relevant supervisory authority is the Swiss Federal Data Protection and Information Commissioner (for transfers subject to the FADP and not the GDPR), or both such Commissioner and the supervisory authority identified in the EU SCCs (where the FADP and GDPR apply, respectively).

9. AUDITS. To the extent required by Data Protection Laws, DocuSign shall make available such information reasonably requested by Customer to confirm DocuSign’s compliance with this DPA (e.g., SOC, ISO, NIST, PCI DSS, similar audit reports issued by a qualified third-party auditor, “**Audit Report**”), or with the Security Attachment for DocuSign Services. Except as provided otherwise in the Agreement or Security Attachment regarding audits, if Customer has a reasonable basis to conclude that an Audit Report provided by DocuSign is not satisfactory to confirm such compliance, Customer may, at Customer’s sole expense, upon thirty (30) days’ prior notice, request an audit during normal business hours of those DocuSign systems and records relevant to DocuSign’s Processing of Personal Data on Customer’s behalf. Customer shall limit its exercise of audit rights to not more than once in any twelve (12) calendar month period.

10. RETURN OR DESTRUCTION OF PERSONAL DATA. Prior to termination or expiration of the Agreement, Customer may retrieve Personal Data processed by DocuSign in accordance with the terms of the Agreement and at Customer’s request, DocuSign will promptly delete or all Personal Data in its possession or control as soon as reasonably practicable, save that this requirement will not apply to the extent that DocuSign is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which Personal Data DocuSign will securely isolate and protect from any further processing, except to the extent required by applicable law. For Personal Data stored in Customer’s service environment, or for the DocuSign Services for which no bulk data retrieval functionality is provided by DocuSign as part of the DocuSign Services, Customer acknowledges that it is required to take appropriate action to back up or otherwise store separately any Personal Data while the DocuSign Services environment is still active prior to termination and acknowledges that if Customer elects to have Personal Data returned, Customer acknowledges that DocuSign does not offer bulk data retrieval as part of the DocuSign Services and Customer will be required to engage DocuSign Professional Services or customer support at a reasonable fee payable by Customer to DocuSign.

11. MISCELLANEOUS PROVISIONS.

Notwithstanding anything else to the contrary in the Agreement, DocuSign reserves the right to make any modification to this DPA as may be required to comply with Data Protection Law so long as any such modification shall not degrade any service functionalities or safeguards associated with providing the DocuSign Services.

Any claims brought under this DPA shall be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

This DPA will remain in force and effect through the term of the Agreement, or for as long as DocuSign is Processing Personal Data subject to this DPA, whichever is longer.

Schedule A

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

The exporter (Controller) is Customer and Customer's contact details and signature are as provided in the Agreement and the DPA.

Data importer(s):

The importer (Processor) is DocuSign, Inc. and DocuSign's contact details and signature are as provided in the Agreement and the DPA.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Any data subjects whose Personal Data is contained in Data Exporter's data being used in the DocuSign Services, as set out in the Agreement which describes the provision of DocuSign Services to Customer, including Customer's Account Administrator, Authorized Users, representatives, and end users, including, without limitation, Customer's employees, contractors, partners, suppliers, customers, and clients.

Categories of personal data transferred:

Any Personal Data that is provided by Data Exporter to Data Importer in connection with the Agreement and the DPA, including, without limitation, contact information such as name, address, telephone or mobile number, email address, and passwords.

Sensitive data transferred (if applicable): N/A.

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

On a continuous basis as needed to provide the DocuSign Services to Customer for the term of the Agreement.

Nature of the processing:

The nature of the Processing is set out in the Agreement between the parties.

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

The purposes of the data transfer are for DocuSign to provide the DocuSign Services pursuant to the Agreement.

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

The data will be retained for the time period needed to accomplish the purposes of Processing, unless otherwise required by applicable law.

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

Please see Section 6 for information about how to access a list of DocuSign's Subprocessors and the nature of the services they provide. All transfers will last for the duration of the Agreement between the parties.

C. COMPETENT SUPERVISORY AUTHORITY

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

The Data Exporter's competent supervisory authority will be determined in accordance with Data Protection Law and, where possible, will be the Irish Data Protection Commissioner.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

See the [DocuSign Binding Corporate Rules](#) and [DocuSign's Security Attachment for DocuSign Services](#).