

## Adobe Sign Additional Terms of Use

Published March 16, 2020. Effective as of April 16, 2020. Replaces all prior versions.

These Additional Terms govern your use of Adobe Sign and are incorporated by reference into the Adobe General Terms of Use ("**General Terms**") located at [www.adobe.com/go/terms](http://www.adobe.com/go/terms) (these Additional Terms and the General Terms are collectively referred to as "**Terms**"). Capitalized terms not defined here have the same meaning as defined in the General Terms. References to "Services" in these Additional Terms are to the Adobe Sign electronic signature services.

### 1. Definitions.

- 1.1 "**Audit Log**" means certain information recorded by us regarding the signing workflow of a particular Electronic Document processed using the Services. The Audit Log may include the date and time an Electronic Document was created, sent, signed, declined, or otherwise modified, or an End User's geographic location as determined by browser or device.
- 1.2 "**Customer Data**" means any data or information not supplied by us that you or End Users import into the Services or transmit via your account.
- 1.3 "**Electronic Document**" means any document uploaded or imported into the Services.
- 1.4 "**End User**" means any individual or company that receives, reviews, accepts, signs, approves, transmits, delegates action to a third party, or otherwise interacts with the Services.
- 1.5 "**Report**" means any graphical or numerical display of Customer Data that contains Adobe's proprietary design, look and feel, which is generated by the Services, including Audit Logs.
- 1.6 "**Transaction**" means each time an Electronic Document, or collection of related Electronic Documents, up to 10 MB or 100 pages are sent to an End User through the Services. Transactions are consumables as described in the VIP Terms.
- 1.7 "**VIP Terms**" means the Adobe Value Incentive Plan Terms and Conditions located at <http://www.adobe.com/go/vip-terms>.

### 2. Term and Termination.

- 2.1 These Additional Terms will continue to apply until terminated by either you or us as set forth in the Terms. In addition to the reasons we may terminate these Additional Terms with you as set forth in the General Terms, we may terminate these Additional Terms if your Services account is used by any unauthorized third parties.
- 2.2 In addition to the sections set forth in the "Survival" section of the General Terms, the following sections will survive any expiration or termination of these Additional Terms: 2.2 (Term and Termination), 3 (Personal Information of End Users), 7 (Storage and Retention of Customer Data), and 9 (Digital Certificates).

### 3. Personal Information of End Users.

- 3.1 **Your Responsibilities.** As between us and you, you are solely responsible for all personal information of End Users used and submitted in connection with the Services. You must:
  - (A) comply with all data protection and privacy laws and rules applicable to personal information of End Users, including obtaining and maintaining consent, where required; and
  - (B) defend, indemnify, and hold us harmless from any claim, suit or proceeding brought against us by an End User in connection with any acts or omissions with regards to personal information of End Users.
- 3.2 **Sensitive Personal Information of End Users.** The Sensitive Personal Information section of the General Terms does not apply to your use of the Services. Notwithstanding the foregoing, in addition to your responsibilities set forth in section 3.1 (Your Responsibilities) above, you specifically acknowledge and agree that in connection with your use of the Services:

(A) you are solely responsible for compliance with the Children's Online Privacy Protection Act of 1998 ("COPPA"), if applicable, including not collecting information from children under the age of thirteen without first obtaining parental consent;

(B) you must not to collect, process, or store any protected health information, electronic or otherwise, pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health ("HITECH"), unless you have entered into a Business Associate Agreement with Adobe; and

(C) you are solely responsible for compliance with the Payment Card Industry Data Security Standard ("PCI DSS"), if applicable. PCI DSS prohibits using the Services to store Sensitive Authentication Data, including Card Verification Code or Value after authorization, even if encrypted. Capitalized terms in this section are defined in the PCI DSS.

**3.3 Emails to End Users.** Adobe sends transactional emails to End Users in connection with the Services on your behalf and in your name as your agent. You are solely responsible for those emails and their contents.

#### **4. License Grants.**

**4.1 License Grant to You.** Subject to your compliance with all applicable terms and your payment of fees, we grant you, during your license term, a non-transferable, non-exclusive and worldwide license to: (A) access the Services through the applicable interfaces; and (B) use and distribute Reports internally within your business, solely for your use of the Services for your internal operations. Unless your applicable sales documentation identifies another Transaction limit, each licensed user is permitted to send up to 150 Transactions during each 12-month license period. Transactions for a given customer account are aggregated among all licensed users, and do not carry over from one 12-month license period to the next.

**4.2 License Grant from You.** You grant us and our affiliates, during your license term, a non-exclusive, worldwide, royalty-free license to use, copy, transmit, sub-license, index, model, store, and display Customer Data, solely to the extent necessary to provide the Services and Reports to you and enforce our rights under the Terms. You grant us and our affiliates a non-exclusive, perpetual, worldwide, and royalty-free license to use, copy, transmit, publish, display, distribute, and aggregate (including combination with similar data of other customers of ours or our affiliates) any anonymous information derived from your use of the Services. Such anonymous data does not include personal information of you or End Users or any data derived from the contents of an Electronic Document.

**5. Customer Usage.** You may use the Services solely for your own business purposes and shall not make your password to the Services available to any third party. You agree that your access and use of the Services is governed by the laws, policies and regulations of individual countries, regions and industries, and it is your responsibility to abide by those laws, policies, and regulations. You agree that you will rely on independent legal counsel to determine the viability of electronic signatures.

**6. End User Terms and Conditions.** The use of the Services is conditioned on each End User accepting the terms of use presented when using the Services, which may include the Consumer Disclosure and Consent terms currently located at <http://secure.echosign.com/public/static/consumerDisclosure.jsp>.

**7. Storage and Retention of Customer Data.** We will store Customer Data so long as the size of that storage does not exceed the amount of storage permitted for your account, if any. We may create reasonable limits on the use and storage of Customer Data, such as limits on file size, storage space, and other technical limits. Customer Data may be deleted if you fail to pay fees due, or if required by law. In the event we delete Customer Data pursuant to this section, we will use commercially reasonable efforts to allow you to transition Customer Data out of the Services, unless prohibited by law. You agree that you are solely responsible for complying with all applicable document retention laws and regulations, including any duty to provide notice to third parties about retention or deletion of documents.

#### **8. Customer Security and Performance.**

**8.1 Your Responsibilities.** You are responsible for configuring and using the security features of the Services to meet your obligations to End Users under applicable privacy, security, and data protection laws and regulations. You are responsible for the security of Electronic Documents that are emailed to End Users from the Services, downloaded from the Services, or which are transferred to a non-Adobe system via an integration feature of the Services. We are not liable for damages arising

out of unauthorized access to your account or to Customer Data if you fail to follow secure password composition, management, and protection practices for your account. We will maintain commercially reasonable administrative, physical, and technical safeguards to help protect the security, confidentiality, and integrity of Customer Data that is under our direct control within the Services. For information about the security certifications applicable to the Services, see: <https://www.adobe.com/content/dam/acom/en/security/pdfs/MasterComplianceList.pdf>.

**8.2 Throttling.** You agree to work with Adobe to create a plan to manage any spikes in demand for system resources driven by your use ("**Spikes**"). In the absence of such collaboration, you agree that Adobe may throttle or otherwise queue your Transactions to manage any such Spikes.

**9. Digital Certificates.** The Services may include technology that allows you to apply digital signatures to PDF documents through the use of digital certificates. The Services also apply a certification signature to PDF documents as a proof of their integrity and origin through the use of digital certificates owned by Adobe. You may not access, attempt to access, circumvent, control, disable, tamper with, remove, use, or distribute such certificates or their corresponding encryption keys for any purpose.