



PSLT - Adobe eSign Services (2015v2)

1. **Content Files.** Customer may use, display, modify, reproduce, and distribute any of the Adobe-provided sample files such as fonts, stock images, sounds or templates (“Content Files”), except Customer must not distribute Content Files on a stand-alone basis. Customer may not claim any trademark rights in, or derivative works of, the Content Files.
2. **Modification.** Adobe may modify or discontinue the On-demand Services or any portions or service features thereof at any time without liability to Customer or anyone else. However, Adobe will make reasonable effort to notify Customer before Adobe makes the change. Adobe will also allow Customer a reasonable time to download Customer Data. If Adobe discontinues an On-demand Service in its entirety, then Adobe will provide Customer with a pro rata refund for any unused fees for that Online Service that Customer may have prepaid.
3. **Third-Party Software Notices.** The creators of certain public standards and publicly available code, as well as other third party licensors, require that certain notices be passed through to the end users of the On-premise Software. These third party notices are located at www.adobe.com/products/eula/third_party/index.html (or a successor website thereto) (“Third Party Notice Page”). The inclusion of these third-party notices does not limit Adobe’s obligations to the Customer.
4. **Storage, Retention and Transition of Customer Data.**
 - 4.1 **Storage and Retention.** Adobe will store Customer Data so long as the size of that storage is not unreasonable in Adobe’s discretion. Adobe may create reasonable limits on the use of Customer Content, such as limits on file size, storage space, processing capacity, and other technical limits. However, Customer Data may be deleted if Customer instructs Adobe to do so, or if required by law. Customer agrees that it is 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.
 - 4.2 **Transition.** If Customer is in compliance with the applicable license terms, Adobe will use commercially reasonable efforts to assist Customer in transitioning Customer Data out of the electronic signature service. The transition must be completed within 30 days of the termination or expiration of Customer’s license to the electronic signature service. At the end of this 30 day transition period, Adobe reserves the right to delete any Customer Data and information relating to Customer’s use of the electronic signature service. Subject to Adobe’s obligation to provide Customer with transition assistance described in this paragraph, upon termination or expiration of the applicable license terms, Customer’s license to the electronic signature service will immediately terminate.
5. **Privacy, Information Security, and Compliance.**
 - 5.1 **Customer’s Responsibilities Regarding Information of Participants.** Customer will comply with (including giving any notifications, obtaining any consents and making any disclosures required under) applicable privacy, security, electronic signature and data protection laws, guidelines, regulations or industry standards or codes applicable to Personal Data of Participants. Customer must obtain and maintain consent from Participants to Customer’s access, use, or disclosure of Personal Data of Participants. Customer must obtain any authorizations from Participants required to enable Adobe to provide the On-demand Service. The use of the electronic signature service is conditioned on Participant acceptance of the terms of use presented when using the electronic signature service.

- 5.2 **Customer Security.** Customer is responsible for configuring and using the security features of the electronic signature service to meet Customer's obligations to Participants under applicable privacy, security, and data protection laws. Customer is responsible for the security of Electronic Documents that are emailed to Participants from the electronic signature service, downloaded from the electronic signature service, or which are transferred to a non-Adobe system via a third party integration feature of the electronic signature service. Customer is liable for damages arising out of unauthorized access to Customer's account or to Customer Data if Customer fails to follow secure password composition, management, and protection practices for Customer's account.
- 5.3 **Privacy and Security.** Adobe will maintain commercially reasonable administrative, physical, and technical safeguards to help protect the security, confidentiality, and integrity of Customer Data. Adobe's collection and use of information in connection with the On-demand Service is governed by the Adobe Privacy Policy (adobe.com/privacy/policy.html).
- 5.4 **Payment Card Industry Data Security Standard (PCI DSS).** The Payment Card Industry Data Security Standard (PCI DSS) prohibits the transmission of any Account Data (including Cardholder Data, Card Verification Code or Value) using the fax signature capability. PCI DSS also prohibits using the electronic signature service 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.
- 5.5 **Health Insurance Portability and Accountability Act ("HIPAA").** Customer is solely responsible for compliance with HIPAA and Health Information Technology for Economic and Clinical Health ("HITECH"). Adobe is not acting on Customer's behalf as a Business Associate, as that term is defined in HIPAA, when providing the On-demand Service.
6. **Legal Counsel. Customer will solely rely on its own legal counsel and determinations as to the use and viability of Electronic Signatures in a particular country or for a particular product or service, and Customer will ensure its use of the On-demand Service conforms and complies with all laws, regulations and policies relevant to a particular country or for a particular product or service.**
7. **Digital Certificates.** Digital certificates may be issued by third party certificate authorities, including Adobe Certified Document Services vendors, Adobe Approved Trust List vendors (collectively "Certificate Authorities"), or may be self-signed. Customer and the Certified Authority are responsible for the purchase, use, and reliance upon digital certificates. Customer is solely responsible for deciding whether or not to rely on a certificate. Unless a separate written warranty is provided to Customer by a Certificate Authority, Customer's use of digital certificates is at Customer's sole risk.
8. **Additional Definitions.**
- 8.1 **"Electronic Document"** means any document uploaded into the electronic signature service.
- 8.2 **"Electronic Signature"** means the capability of the electronic signature service to include an electronic sound, symbol, or process attached to or logically associated with an Electronic Document and executed or adopted by a person with the intent to sign the Electronic Document
- 8.3 **"Participant"** means a individual or entity that electronically reviews, accepts, signs, approves, transmits, or delegates action to a third party regarding Electronic Documents via Customer's electronic signature service account.