Federal Trade Commission
Privacy Impact Assessment

Adobe Sign

February 2025

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC) strives to protect consumers from fraudulent, deceptive, and unfair practices in the marketplace. To accomplish this mission, the FTC conducts investigations, takes law enforcement action against those breaking the law, develops rules to maintain a fair marketplace, conducts research and issues reports to shed light on important issues, and educates consumers and businesses about their rights and responsibilities. The FTC monitors changes in the marketplace, evaluates emerging practices, and identifies consumer protection issues associated with the use of technology. FTC staff often collect declarations from consumers and external parties, and coordinate with them to obtain signatures on official papers and legal documents. In order to ensure that such transactions are completed in an efficient and secure manner, the FTC collects digital signatures through Adobe Sign.

Adobe Sign is a Fed-RAMP authorized cloud-based signature service that allows the user to share, sign, track, and manage signature processes using a computer or mobile device. It allows the FTC to simplify the process of obtaining a signature on documents for legal and administrative tasks, including consumer declarations and myriad other transactions requiring signatures as part of the FTC's business functions. Adobe Sign expedites the signature process by removing the time-consuming mailing operation and physical exchange of documents.

FTC staff and contractors upload data to Adobe Sign that has been created or obtained in connection with the Commission's law enforcement, policy, and other activities. User-created content may also include declarations, contracts, employment documents, or other artifacts necessary to support the FTC mission. The documents requiring signature may include any and all types of data, including PII and sensitive information.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The information in this system is collected, maintained, and disseminated pursuant to the Federal Trade Commission Act, 15 U.S.C. §§ 41-58, and other laws and regulations the Commission enforces.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☐ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☒ Home Address	☒ Photographic Identifiers (e.g., image, x-ray, video)	☐ Employment Status, History, or Information
☒ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☒ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☒ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: Documents uploaded may contain any and all types of PII
☒ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

Although the documents shared for signature via Adobe Sign can contain any and all types of PII, typically the FTC collects only the recipient's name, email address, and phone number for use in Adobe Sign. Occasionally, the recipient's home address and/or a picture of a government-issued ID may be required for verification purposes. Financial information, if relevant and collected by the FTC, is limited to the recipient's bank name and/or the last four digits of their account number.

For administrative users of Adobe Sign (FTC employees and contractors), the following data elements are collected: full name, email address, work address, work phone numbers, User ID, and PIN/password.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

The FTC houses a variety of non-PII information in Adobe Sign depending on the needs and purposes of the offices that use this software. Documents that could be in Adobe Sign may

[1] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

include a variety of law enforcement documents, internal staff memoranda, human resource documents, and other documents containing both public and nonpublic information as needed to support the FTC mission. Adobe Sign may collect additional information such as the exact date and time an Adobe Sign agreement was opened. The initiator of the agreement can request a photo ID be uploaded for verification purposes.

2.3 What is the purpose for collection of the information listed above?

Information in Adobe Sign is collected, used, disseminated, and maintained for the Commission to perform its law enforcement, policy, personnel management, and other activities. Due to the range of supported services, personal information may be present for a variety of reasons within Commission papers, court records, human resources files, and any other document(s) needed to support the FTC mission.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	*Type of Data Provided & How It Is Collected*
FTC Staff	FTC staff and contractors upload data that has been created or obtained in connection with the Commission's law enforcement, policy and other activities. User-created content may also include declarations, contracts, employment documents, or other artifacts necessary to support the FTC mission. These documents may include any and all types of data, including PII and sensitive information. FTC users are required to provide the following information in order to create an account and use Adobe Sign: Username, Full Name, Office/Division, phone number, and work email address. When initiating the signature process, FTC staff must enter the recipient's email address and phone number.
External Parties (Signatories)	In order to electronically sign a document, the recipient is required to log on to Adobe Sign using their email address and phone number. Other information such as the recipient's mailing address or photograph of a government issued identification card may be required. This information is used to verify the recipient's identity and to complete the signature process.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
FTC Staff	Access to Adobe Sign is restricted to authorized FTC end users. All end users must adhere to the FTC Rules of Behavior. Access to the information stored within Adobe Sign is dependent on the particular business purpose and the access permissions granted to a specific user. For example, system administrators may have access to system data and system audit logs in order to manage access roles, monitor system usage, perform system audits, and complete other necessary job functions.
Members of the Public (Signatories)	FTC staff require signatures from members of the public (signatories) for contracts, declarations, administrative documents, and other documents necessary to complete the FTC mission. Signatories only have access to the document(s) that require their signatures.
Contractors and/or Service Providers	FTC may have contractor support within program areas and these contractors will have access to the information in Adobe Sign as required to perform their duties. Adobe staff will not have access to FTC documents unless access is approved by the FTC. This access may be granted for e-discovery or technical support purposes. FTC staff have full control of who can access data and documents in Adobe Sign.
Office of Inspector General (OIG)	Under appropriate circumstances, data in Adobe Sign or Adobe Sign log data may be provided to the OIG for auditing or law enforcement purposes.

3.2 Do contractors and/or third-party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Authorized FTC contractors have access to information in Adobe Sign, when necessary. Some authorized FTC contractors have access to Adobe Sign simply as users, and a small number of authorized FTC contractors have access to certain administrative functions.

All FTC contractors are required to sign NDAs and complete the FTC's Information Security Awareness and Privacy training prior to obtaining access to any FTC systems, and annually thereafter to maintain network access and access to those systems.

Adobe staff do not have access to FTC documents unless access is approved by the FTC. This access may be necessary for e-discovery or support request purposes. FTC staff have full control of who can access what data and documents in Adobe Sign.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third-party service provider.

Contractors who access Adobe Sign are subject to the same rules and policies as FTC staff. Contractors must also follow the reporting and other procedures in the FTC's Breach Notification Response Plan.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

Wherever possible, the FTC provides timely and effective notice to the public and/or to individuals about activities that impact privacy. For information that is collected pursuant to a request from the FTC, notice is provided as part of that request. The FTC's Privacy Act statements are included on all forms, websites, and other instruments by which Privacy Act information is collected from individuals, either in written or oral form. For those occasions where the FTC cannot provide notice at the time the information is collected (e.g., when the information is collected by another law enforcement agency or another organization), the FTC provides notice via its Privacy Policy, its Privacy Act system of records notices (SORNs), and its PIAs, including this one. Users would be informed that their information will be placed into Adobe Sign when it is collected by the FTC employee collecting it and working with them to collect their signature.

☒ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☒ Written ☐ Oral)
- ☒ FTC Website Privacy Policy
- ☒ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☒ Other (*explain*): Individual notified by the FTC employee they are working with to collect their signature in a document.

☐ Notice is not provided (explain): _____

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

The opportunity or right depends on how the information is collected. The FTC uses Adobe Sign to collect signatures from members of the public in furtherance of the FTC's law enforcement activities and/or policy mission. The information that is needed from signatories in order to authenticate their identities is generally collected beforehand by FTC staff via

phone, email, or in person. Only what is absolutely necessary to complete the signature process is placed into Adobe Sign. The person receiving the request to sign a document through Adobe Sign can decline to sign electronically; however, that may result in significant delays or failure to complete the signature process altogether. The data that is uploaded to Adobe Sign resides in the system for up to 30 days, after which it is automatically deleted.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Individuals may request access to federal agency records or information through Freedom of Information Act (FOIA) requests (with the exception of certain types of records). The Privacy Act allows most individuals to seek access to federal agency records about themselves and affords that person the right to challenge the accuracy of the information contained about them. Specify if there are procedures in place to allow individuals access to their own information and how they are provided with access. The individual signing a document in Adobe Sign is not required to create an account in order to complete the requested action(s).

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

Members of the public do not have direct access to their own information in the Adobe Sign system and therefore cannot change or edit their own information. If the document recipient notices an error or inaccuracy in the documents provided to them for signature, they must contact the FTC employee (sender) directly and detail any corrections that need to be made. Once the information has been corrected by FTC staff, the document will be sent over once more to the recipient for signature.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up to date?

Information that is used by the FTC as part of its law enforcement and other activities is reviewed for accuracy and timeliness as required by the particular activity and the laws and authorities, if any, applicable at the time the agency compiles the records (e.g., FTC Act, personnel laws, administrative or court evidentiary rules and procedures).

The individual signing the document in Adobe Sign has the opportunity to review the document for accuracy prior to signing it. The person can refuse to sign the document and/or recommend necessary changes to make the document more accurate prior to signing it.

System administrators ensure FTC user information is complete and accurate for access control through Active Directory (AD) authentication but will not ensure that data created or entered by external users (signatories) is complete, accurate, or current. AD is updated immediately when a user account is disabled or terminated. User contact information is removed once the user account is deleted. Within the FTC, users have the ability to enter their own information and to ensure that it is current.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

FTC's Adobe Sign application is not accessible to anyone outside the FTC. The principle of least privilege is used to grant access to FTC staff and contractors, and user actions are tracked in the Adobe Sign audit logs. All potential FTC staff and contractors are subject to background investigations and suitability reviews in accordance with OPM and DCPA (Defense Counterintelligence and Security Agency) guidance. Before accessing Adobe Sign, these individuals must first attend new employee orientation and successfully complete the FTC's Information Security Awareness and Privacy training. All staff must annually acknowledge procedures for handling PII – including minimizing PII – and attest that all PII maintained by the individual has been properly secured and accounted for as part of the FTC's Information Security Awareness and Privacy training.

Additionally, Adobe Sign is limited to the people who need to use it for authorized business purposes. FTC's instance of Adobe Sign is integrated with the FTC's OKTA system to limit who has access to the system.[2] Users would watch a training video created by Adobe Sign to learn how to use the system. Documents will be placed into Adobe Sign by the FTC user for the purpose of review and signature by the intended recipient.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

The FTC does not use PII to conduct Adobe Sign system testing, training, or research.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

Information in the FTC Adobe Sign cloud instance is retained for 30 days and then destroyed in accordance with applicable FTC policies and procedures. FTC staff are responsible for transferring any records created within Adobe Sign from the cloud to the FTC's secure network and preserving such records in accordance with the applicable FTC records retention

[2] For more information on OKTA, see the OKTA Privacy Impact Assessment available online.

schedule approved by the National Archives and Records Administration (NARA). FTC staff receive training and reminders about their records retention and destruction obligations. All information is securely and irreversibly disposed of/destroyed in accordance with applicable FTC policies and procedures, OMB, NARA, and NIST regulations and guidelines.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

Yes. When an FTC employee initiates the Adobe Sign process, an email message is sent to the recipient with a link to the document that requires signing. Once the recipient clicks on the link, they are directed to a secure website where they can validate their identity and provide their digital signature. The Adobe website uses session cookies to facilitate the user's signing and to prevent the website from timing out while a user is logged into the document. The FTC does not have access to the cookie data collected by Adobe Sign.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	***Mitigation Strategy***
Misuse of data by authorized users	Prior to receiving access to the FTC's network, all users must agree to the FTC Rules of Behavior, which includes consent to monitoring and restrictions on data usage.
Unauthorized system access	All users must have an FTC account and government-issued personal identity verification (PIV) card to access Adobe Sign. FTC's user identity management process includes authentication with Active Directory (AD) to control and manage access restrictions to authorized personnel on an official need-to-know basis. The FTC utilizes a combination of technical and operational controls to reduce risk in the Adobe Sign environment, such as encryption, passwords, audit logs, firewalls, malware identification, and data loss prevention policies. As a FedRAMP-approved cloud service provider, Adobe Sign undergoes regular reviews of its security controls. Data sent to third parties using Adobe Sign will use email and phone number for authentication to ensure the document(s) is only accessed by the authorized third party.

Risk	*Mitigation Strategy*
Unintentional Sharing with Unauthorized Recipient	In the event that an FTC staff person unintentionally sends the Adobe Sign link to the wrong email address, the unintended recipient will be able to view and sign the document, unless the sender updates the link to by using the "Replace Recipient" feature. This mitigation strategy must be enacted prior to the unintended recipient signing the document.
Data Leakage	The contract between FTC and Adobe Sign does not allow the service provider to access, review, audit, or transmit FTC data without its permission. Data placed into the Adobe Sign system is held for 30 days, after which it is downloaded to the FTC system, and subsequently deleted from Adobe Sign's system.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

FTC user access is managed through the FTC's Active Directory (AD) infrastructure, which uniquely identifies, authenticates, and applies permissions to authorized user sessions based on FTC policies and procedures. This allows the FTC to leverage organizational multifactor authentication solutions, including FIPS-201 compliant PIV cards, already deployed to meet internal identification and authentication requirements. The use of AD also allows automatic enforcement of certain policies and requirements, such as password complexity and maximum log in attempts, for FTC users. The system also uses OKTA, which will not allow an FTC employee access or use Adobe Sign if they are not authorized to do so. Users are also locked out after three invalid logon attempts.

Additionally, FTC security policies require automated monitoring of information system components with regard to flaw remediation. Data sent to third parties using Adobe Sign use email and phone number for authentication to ensure the document(s) is only accessed by the authorized third party.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

Adobe Sign does not itself require a SORN; however, SORNs that cover documents and records in Adobe Sign that are considered part of Privacy Act systems are accessible at https://www.ftc.gov/site-information/privacy-policy/privacy-act-systems.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

The administrative and technical controls described in section 5.2 of this document provide assurance that the collection, use, and maintenance of the information will be conducted as described in this PIA. This PIA aligns with the FTC's existing privacy policies and procedures.