Adobe Sign

Adobe

WHITE PAPER

Adobe Sign

An Analysis of Shared Responsibilities for 21 CFR Part 11 and Annex 11 Compliance

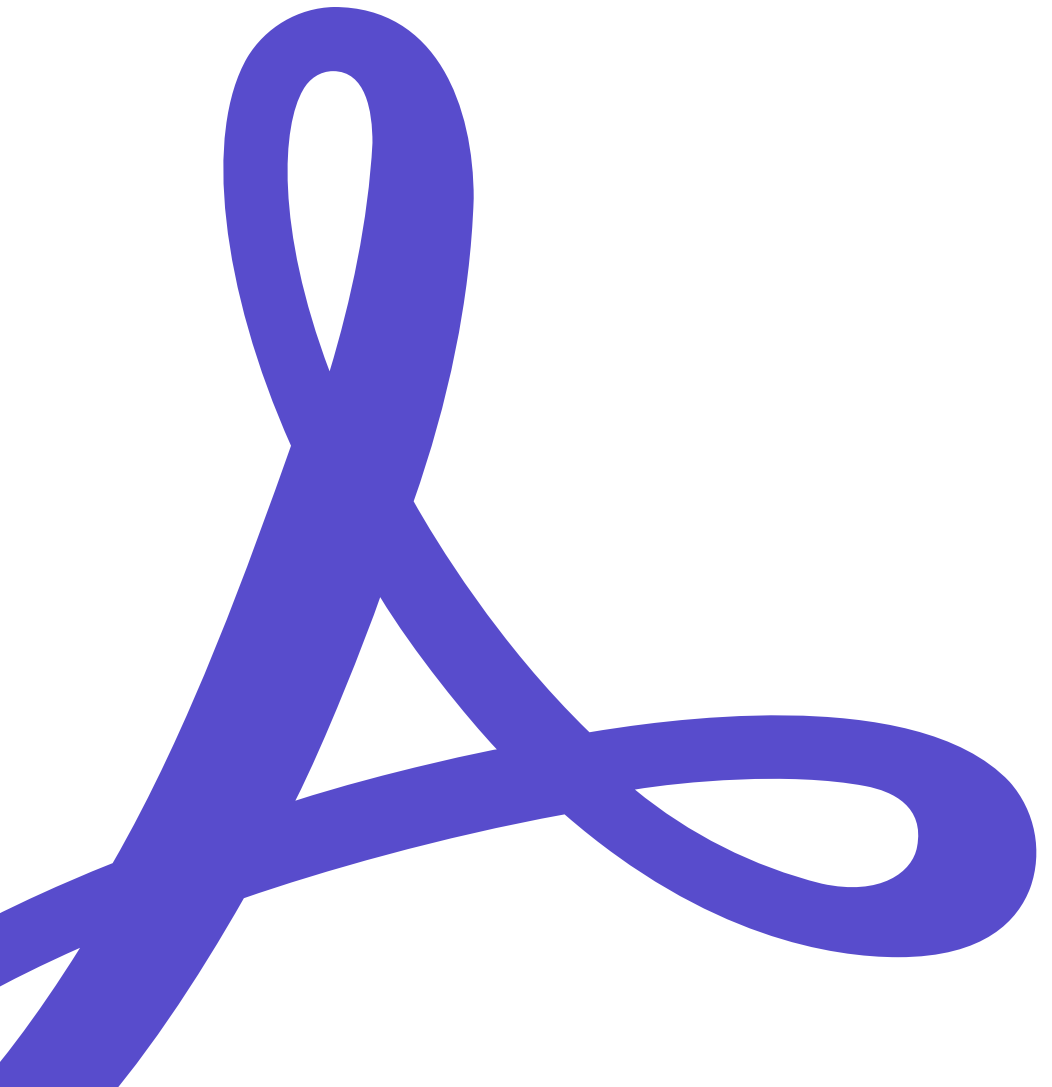

Table of Contents

1 Introduction

While increasingly more Healthcare and Life Science organizations are benefiting from the advantages of digital document management, these companies must adhere to strict regulatory requirements if using computer systems to generate and manage electronic records and electronic signatures in the place of paper-and-ink-based records.

Each jurisdiction has its own set of rules, but all have the common interest of ensuring electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records and hand-written signatures.

- **21 CFR Part 11:** Under the United States (U.S.) Code of Federal Regulations, 21 CFR Part 11 provides requirements for electronic records and electronic signatures.
- **Annex 11:** Under the European Union (EU) EudraLex rules and regulations governing medicinal products, Volume 4 Annex 11 establishes the conventions for using computerised systems.

Adobe Sign is a cloud-based electronic signature service that allows users to implement automated electronic signature workflows in place of traditional paper-and-ink signature processes. With Adobe Sign, electronic signature requests are emailed to signers with unique hyperlinks to documents and added security measures (such as user authentication and password-protection) are possible. Cloud signatures can be used to apply a certificate-based digital signature, such as advanced or qualified e-signatures as defined by the EU eIDAS regulation. If implemented properly, it is possible to satisfy 21 CFR Part 11 and Annex 11 requirements when using Adobe Sign to execute electronic signatures.

This paper presents an analysis of the technical features and the procedural controls that allow for the application of compliant signatures using Adobe Sign. This assessment focuses on how Adobe and the organization using Adobe Sign share responsibilities for achieving compliance.

2 Scope and Audience

While various use cases are possible with Adobe Sign, this paper pertains to the use of Adobe Sign for the application of electronic signatures to controlled GxP documents in a manner that is 21 CFR Part 11 and Annex 11 compliant.

This paper focuses on the Adobe Sign electronic signature service. The use of Adobe Acrobat and Reader for desktop certificate-based signatures and PDF signatures is not covered in this document.

The intended reader of this paper is the Healthcare and Life Science organization using Adobe Sign as part of a GxP regulated process ("customer").

Electronic signatures are a way to indicate consent or approval on digital documents and forms. A digital signature is a specific implementation of an electronic signature that uses a certificate-based digital ID to verify the signer's identity and binds the signature to the document with encryption. Adobe Sign supports both electronic signatures and digital signatures. Since a digital signature is a type of electronic signature, the term "electronic signature" will be used throughout this document when evaluating the Adobe Sign services.

3 Background

3.1 Adobe Sign System Overview

Adobe Sign, an Adobe Document Cloud solution, is a cloud-based electronic signature service offered in a Software-as-a-Service (SaaS) model managed by Adobe (the service provider). The configuration of the Adobe Sign services with the settings needed for the customer's business processes is managed through their Adobe Sign account.

Licensed users must be added to a customer's Adobe Sign account. Electronic signature functionality is made available to active, fully enabled users within the Adobe Sign account (internal users). Active internal users are authorized to use electronic signature functionality based on the privileges assigned to them in Adobe Sign (e.g. sending and/or signing privileges). A sender may upload a document in the Adobe

Sign portal and send an email notification to inform each signer that the document is available for signature. Invited signers can access and sign the document from any device through a secure web browser session.

The Adobe Sign application can be configured to use single or multi-factor authentication methods to verify the signer's identity, with options to do so at various points in time (e.g. upon system login, upon opening an agreement to view the document, and when applying a signature).

Once all requested electronic signatures have been applied to a document, the system can be configured to send a hyperlink for the signed record to the individual who sent the document for signature and to all signers. Internal users can access the signed record via the hyperlink or directly from the Adobe Sign portal. As external users do not have access to the Adobe Sign account, they can access the signed record via the hyperlink only.

For each signed record, an audit report is created. The audit report includes the identity of each signer and a timestamp indicating the date and time at which the electronic signature was applied. The signed record and its audit report are available in PDF format and are certified using public key infrastructure (PKI) digital certificates. These can be retrieved for retention in a system used by the customer to manage electronic records, e.g. electronic document management system (EDMS).

Transactional data (including original documents, workflow events, and final signed PDF documents) are securely stored within the data layer (databases and file store) managed by Adobe. The Adobe Sign infrastructure resides in top-tier data centers managed by trusted cloud service providers. Additional information related to the Adobe Sign system architecture and governance processes is provided in the Adobe Sign Security Overview White Paper.

Backed by numerous security features, processes, and controls, Adobe Sign is compliant with rigorous security standards, including SOC 2 Type 2, ISO 27001, and PCI DSS. For additional technical details on applicable information system controls in place, the latest Adobe Document Cloud SOC 2 Type 2 attestation report is available upon request from Adobe account representatives.

It is the responsibility of the customer using Adobe Sign as part of a GxP regulated process to evaluate system features and to select options that meet their business needs. The customer must also implement appropriate processes and safeguards to govern their business activities.

3.2 Adobe Sign Identity Management

Identity management is fundamental to obtaining a legal signature, as the falsification of one's identity results in a fraudulent signature. A strong identity verification process is required to establish a trustworthy link between who someone claims to be and who they really are.

Identification is the act of presenting some record or qualifying personal information to confirm a person's existence. This is usually performed just once, by validating an official ID document or other piece of personally identifiable information. Typically, this verification is carried out by the customer or a trust service provider (TSP) and, pursuant to 21 CFR Part 11.100(b), is done prior to assigning an individual the credentials needed to identify themself to the Adobe Sign service.

Identity authentication is the process of confirming that a person is who they claim to be. Methods for authenticating users generally rely on at least one of the following: something you have (e.g. smart card), something you know (e.g. password) something you are (e.g. biometrics). A person's identity must be authenticated each time they access a system or resources.

Adobe supports the following identity types:

- Adobe ID is for Adobe-hosted, user-managed accounts. The individual user creates, owns and manages the ID.
- Enterprise ID is for Adobe-hosted, enterprise-managed accounts. The organization (customer) creates, owns and manages the ID. User accounts can be created on verified domains.

- Federated ID is for enterprise-managed accounts. The organization (customer) creates, owns and manages the ID. Additionally, the organization (customer) manages user credentials and uses Single Sign On (SSO) via a SAML 2.0 compliant identity provider.

Adobe Sign supports several different choices to authenticate users. Users can be those who use the application to send documents (and have a Sign licence) as well as those who access documents that were sent to them for their signature. Because most users have unique access to one email account, the first level of identity authentication to Adobe Sign is achieved by sending an email request to a specific person.

- Adobe Sign authentication — This option requires signers to log in with an account created with Adobe. Because Adobe Sign uses email as a delivery mechanism, the Adobe Sign authentication method used on its own is considered single factor authentication.

The authentication is rendered more robust and secure when an additional method (i.e. multi-factor authentication) is used. The following second-factor authentication methods are available in Adobe Sign:

- Password based authentication — This option requires that the signer enter a unique password before being allowed to sign a document.
- Phone authentication — This option requires signers to enter a verification code that is sent to their phone via SMS or voice call before being allowed to sign a document.
- Knowledge-based authentication (KBA) — This option provides a higher level of authentication in which the signer is asked a number of personal questions, e.g. "What is your mother's maiden name?". The signer must answer all questions correctly before being allowed to sign a document.
- Government ID authentication — This method instructs the recipient to supply an image of a government-issued document (Driver's license, Passport) and evaluates the authenticity of that document.

Additionally, Adobe Sign may be used in conjunction with Adobe-approved trust service providers to verify signer identity.

Users with administrative privileges can configure a customer's account to mandate the use of a specific method to verify the signer's identity. Different authentication controls can be configured to accommodate internal and external recipients. Before they can sign a document, the signer is prompted to confirm their identity using the authentication method that is chosen for this recipient type.

Adobe Sign uses a role-based model to control authorization and system access. Users with administrative privileges can add individuals as Adobe Sign users to the customer's account and can assign roles (Signer, Sender) to grant signing and sending authority to select individuals within their account.

For additional technical details, see the Adobe Identity Management Services Security Overview.

3.3 Key Terms

Agreement	The customer-facing object that Adobe Sign creates from the uploaded files (documents) that are routed for signature. "Agreement" is the term used to define both the object during the process of obtaining signatures and the final PDF that is generated. Note: A signed agreement is used interchangeably with the term "Record".
Customer	Members of a health or life science organization using Adobe Sign as part of a GxP regulated process
GxP	Set of compliance regulations including but not limited to, Good Clinical Practice (GCP), Good Laboratory Practice (GLP), Good Manufacturing Practice (GMP), Good Distribution Practice (GDP), and Good Pharmacovigilance Practice (GVP)
Public key infrastructure (PKI)	A technology approach for the creation, storage, distribution, and revocation of digital certificates which are used to verify that a specific public key belongs to a particular entity (person or organization).
Recipient	An individual assigned a request to apply an electronic signature to a document. The recipient may be designated as internal or external, as follows: • An internal recipient is any active user (as identified by the email address) within the same Adobe Sign account from which the agreement was sent and who is the recipient of a request to apply an electronic signature. Internal recipient may be used interchangeably with internal signer or internal user throughout the document. An internal user is not per se someone who has an email address from the customer's email domain. • An external recipient is any individual whose email address is not included in the account-level user list and who is the recipient of a request to apply an electronic signature. External recipient may be used interchangeably with external signer or external user throughout the document.
Record	An agreement that has been signed by all required Signers.

4 Conformance with Regulations

In this section, the compliance requirements of 21 CFR Part 11 and Annex 11 are evaluated to determine how the Adobe Sign cloud service conforms with the regulations. In addition to Adobe Sign technical controls, the organization using Adobe Sign as part of a GxP regulated process ("customer") is responsible for defining and implementing processes to ensure that Adobe Sign is used in a controlled manner that meets the regulatory requirements.

4.1 21 CFR Part 11

21 CFR Part 11 defines the requirements for electronic document and signature submissions to the U.S. Food and Drug Administration (FDA). This law specifically details FDA regulations for *"electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper."* 21 CFR Part 11 mandates that life science organizations using electronic signatures meet three distinct categories of compliance requirements:

1. Security for "closed systems" (Subpart B, Sec. 11.10)
2. Security for "open systems" (Subpart B, Sec. 11.30)
3. Requirements for executing an electronic signature (Subpart B, Sec. 11.50 and Sec. 11.70; Subpart C)

Under 21 CFR Part 11, a "system" is described as either closed or open. A closed system is an environment in which system access is controlled by the individuals who are responsible for the content of the electronic records that are in the system. Conversely, an open system is an environment in which system access is not controlled by individuals who are responsible for the content of electronic records that are in the system. Adobe Sign is generally considered to be an open system; however, customers can also create a closed system for their organization if the customer has administrators who manage system access and the individual users are responsible for the content of the electronic records.

Regulations (21 CFR Part 11)

Subpart B — Electronic Records

Sec. 11.10 Controls for closed systems.

What the law requires

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

Subsection 11.10 (a)

What the law requires	How Adobe Sign complies	Customer Responsibilities
Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Adobe complies with accepted standards and IT best practices, as assessed through SOC 2 Type 2 reporting and ISO 27001 certification. Processes are in place to ensure Adobe systems are adequately tested as part of the development lifecycle. Risk management is incorporated into processes surrounding the development and maintenance of Adobe Sign. Test coverage includes common use cases, and testing must be completed successfully prior to releasing software updates. A Quality Certificate is produced for every major software release as an attestation that the release complies with Adobe's quality standard for software development. Changes to the Adobe Sign services are planned and communicated by Adobe prior to implementation of the change. Critical contacts named for an Enterprise or Business customer account may receive pre-release communications by email on a quarterly basis, directing customers to the pre-release notes. The email communications are sent 60, 30, and 15 days before release and again on the day post release. Adobe maintains the Adobe Sign services in a secure and controlled state. Third parties to whom any infrastructure services are outsourced must undergo strict evaluation (per Adobe's vendor assessment program). Processes have also been implemented to govern backup management and system monitoring.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Defining their business process needs (intended use). • Performing validation activities (with documented evidence) to demonstrate that Adobe Sign is fit for the customer's intended use of the system and meets regulatory requirements. Procedural controls should be implemented to define the validation approach in the context of GxP regulatedactivities. • Implementing procedural controls to govern the controlled operation of the system and how changes are made to the Adobe Sign account configuration. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

Subsection 11.10 (b)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	Once all electronic signatures have been applied to a document using Adobe Sign, the system can be configured to send a hyperlink for the signed record to the sender and to all signers for download. Internal users can access the signed record via the hyperlink or directly from the Adobe Sign portal. External users can access the signed record via the hyperlink only. The signed record and its audit report are made available in PDF format and can be viewed with a PDF viewer. These PDFs are certified and sealed, providing proof of origin and integrity. Users with appropriate permissions can download a signed agreement and its audit report from Adobe Sign for retention in a system used by the customer to manage electronic records, e.g. Electronic Document Management System (EDMS). Customers can retrieve their data from the Adobe Sign services throughout the duration of their contract with Adobe, unless a Privacy Administrator deleted an agreement or data governance policies and retention rules are defined. Retention rules specify the timeframe after which transactions, agreements, and the supporting audit and personal data can be automatically deleted from Adobe Sign.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing data repatriation process(es) for moving signed records and the associated audit reports back to a customer-managed EDMS. The process for retrieval of records from the Adobe Sign services should include provisions to verify that these are certified by Adobe. • Assessing the customer's EDMS used to retain signed records to ensure compliance to this regulation.

Subsection 11.10 (c)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Adobe complies with accepted standards and IT best practices, as assessed through SOC 2 Type 2 reporting and ISO 27001 certification. Processes have been implemented to govern backup management and disaster recovery. Adobe Sign's hosting environment is designed to withstand service disruptions. Multiple cloud providers are used and multiple geographically dispersed cloud regions are leveraged to provide failover capability. Processes are in place to ensure the cross-region failover and failback capability is tested. As part of Adobe's Business Continuity and Disaster Recovery (BCDR) program, disaster recovery testing for Adobe Sign is conducted on an annual basis and results are documented. All Adobe Sign documents (electronic records) are encrypted using PCI DSS approved encryption algorithms and stored securely within the data layer (databases and file store) managed by Adobe. The Adobe Sign infrastructure resides in top-tier data centers managed by trusted cloud service providers. A complete audit history is created for each agreement, including dates, times, and who accessed documents. The signed record and its audit report are made available in PDF format, which can be retrieved and extracted (downloaded) from the Adobe Sign service for retention in a system used by the customer to manage electronic records, e.g. Electronic Document Management System (EDMS).	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices. • Implementing appropriate backup infrastructure and policies for records retrieved from the Adobe Sign service and retained in the customer-managed EDMS. The backups must be periodically tested. Archiving policies must be established to ensure availability of the data throughout the retention period. • Assessing the customer's EDMS to ensure compliance to this regulation.

Subsection 11.10 (d)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Limiting system access to authorized individuals.	Adobe Sign allows users with administrative privileges to add authorized users to an Adobe Sign account and groups. Only administrators can access the areas of the system where account administration and configuration activities are performed. User entitlement can be managed from within the Adobe Sign account or through the Adobe Admin Console. Adobe offers different identity types to authenticate and authorize users: Adobe ID, Enterprise ID, Federated ID. If using Federated ID, it is possible to integrate the organization's enterprise directory services with the Adobe Admin Console, facilitating the automated creation, update and removal of user accounts and user entitlement in Adobe Sign. The customer's Adobe Sign account can be configured to mandate the use of a specific method to verify the signer's identity. Different authentication controls can be configured to accommodate Internal and External recipients. Regardless of ID type preferred by customer, internal users are required to authenticate themselves using valid credentials (email address and password) based on the identity type chosen for the customer's Adobe Sign account. When the account is configured to use Federated IDs, internal users will be able to authenticate via Single Sign On (SSO). For External recipients, Adobe Sign can be configured to require External signers to authenticate using the following authentication methods, which can be selected by the sender when setting up the agreement: • Adobe Sign authentication, or • Phone authentication (Although other authentications mechanisms are possible, they are typically not used for 21 CFR Part 11 implementations of Adobe Sign.) Valid credentials are required to log into the Adobe Sign service (for internal users). External signers do not gain access to the Adobe Sign portal. External users gain access only to the agreements which they are requested to sign. The system can be configured to require all signers to provide valid credentials (according to the specified identity verification method) before accessing the document for signature and at the time of signing (Click to Sign). If using certificate-based digital signatures, the system will request additional credentials (e.g. personal identification number (PIN) or one-time password (OTP)) issued from a trust service provider at the time of signing. Adobe complies with accepted standards and IT best practices, as assessed through SOC 2 Type 2 reporting and ISO 27001 certification. Processes are in place to ensure physical and logical security measures are implemented. Adobe engages with third party security firms to regularly perform penetration testing to uncover potential security vulnerabilities. The Adobe Sign security team evaluates security vulnerabilities and implements mitigation strategies to mitigate threats and to improve overall security of the Adobe services. Adobe maintains segmented development (for product development activities) and customer-facing production environments for Adobe Sign. Network and application-level access is controlled. Employees with no legitimate business purpose are restricted from accessing these systems.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process for user access management, including clear criteria for granting/revoking user access and how access requests are documented. • Configuring the system in a manner that enforces user authentication to restrict system access. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and best practices regarding logical and physical security. Additionally, a customer using Adobe Sign's digital signature functionality is responsible for performing the initial assessment and periodic re-evaluation of the chosen trust service provider to ensure signature authenticity.

Subsection 11.10 (e)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	Adobe Sign generates an audit trail capturing the history of activities for each agreement. This audit trail functionality cannot be disabled by the customer. The audit trail can be retrieved as an audit report in PDF format and can be viewed with a PDF viewer. The audit report is associated to the signed document and these are linked together through the Transaction ID of the agreement on the Adobe Sign server. The audit report and the associated signed document can be retrieved as two distinct PDF files or merged into a single PDF file. The PDF is certified with a digital certificate owned by Adobe, providing proof of origin and integrity of the audit trail and to prevent tampering. The audit report captures each signature event, including the identity (full name and email address) of the user who electronically signed the document. Actions recorded in the audit report are sequential and do not obscure previous audit trail entries. All entries are date and time-stamped using Adobe server time. The time stamp is applied when the Signer presses the Click to Sign button. The audit report also captures the identity of a user who decides to reject the document or cancel the signature process. An authorized user (sender) may upload a document in the Adobe Sign portal. If not already in PDF format, Adobe Sign will convert compatible file formats into PDF format prior to sending a document for signature. Once the agreement is in process (as of when the first recipient completed their signature), the document in PDF format cannot be modified. As a result, actions that modify electronic records are not presented in the audit report. Retention rules can be configured to define the timeframe after which transactions, agreements, and the supporting audit and personal data can be automatically deleted from the Adobe Sign service. When creating a retention rule, it is possible to define a distinct retention period for the associated audit trail. If this option is not enabled, the audit record will not be deleted.	Signature field(s) are added in the document for each expected electronic signature. Additional agreement field(s) may also be added (e.g. information fields, data fields). The inclusion and completion of additional fields is not captured within the audit trail. The customer is responsible for defining processes under which the inclusion of additional fields is permitted. An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process for retaining, backing up and archiving signed records and the linked audit reports, including provisions to verify that PDF documents retrieved from Adobe Sign are certified by Adobe. • Defining the business processes utilizing Adobe Sign to specify if it is permitted to include additional agreement fields (other than the signature field) when preparing the document for signature.
Subsection 11.10 (f)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	An agreement may be sent to one or multiple signers. Adobe Sign can be configured to allow for sequential signing, where signatures are applied in a predefined order. The order in which signatures are applied is enforced on a per document basis, with the Sender having the authority to select the signing order. The system can also be configured to allow for assigned signers to apply signatures in parallel with no enforced sequence.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Defining the business processes utilizing Adobe Sign to specify any mandatory signature sequences. • Configuring the system in a manner that is consistent with the signature sequences that are required by the business processes.

Subsection 11.10 (g)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	Adobe Sign uses a role-based model to control authorization and system access. Users with administrative privileges can add individuals as Adobe Sign users to the customer's account and can assign roles (Signer, Sender) to grant signing and sending authority to select individuals within their account. Higher level administrative functions can also be assigned to specific users. Only administrators can access the areas of the system where account administration and configuration activities are performed. Prior to sending a document for signature, a signature field is added in the document as a placeholder for each expected electronic signature. An authorized signer can only access and apply their electronic signature in the signature field that is associated to them.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Configuring the system in a manner that enforces user authentication to restrict system access. • Implementing a process for user access management, including clear criteria for providing/revoking user access and how access requests are documented. • Implementing a process to govern the use of Adobe Sign for the application of electronic signatures. • Implementing a process to ascertain the identity of External signers prior to assigning them signature requests and to provide guidelines to the sender for determining the appropriate mode of authentication.
Subsection 11.10 (h)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Users can access the Adobe Sign service from any device via a secure web browser session. In the context of this assessment, the Adobe Sign service is used for the application of electronic signatures to controlled documents. Adobe Sign is not used to input data. If needed, compliance to this regulation is achieved through customer-implemented controls.	Device checks are warranted in an environment where only certain devices have been selected as legitimate sources of data input or commands. In such cases, the device checks would be used to determine if the data or command source was authorized. If deemed necessary, an organization using Adobe Sign as part of a regulated process is responsible for: • Determining whether the implementation of device checks is required based on the regulatory impact and associated risks. • Defining the process governing which devices are authorized to provide data or operational instructions, including the implementation of necessary controls.

Subsection 11.10 (i)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Determination that persons who develop, maintain, or use electronic record/ electronic signature systems have the education, training, and experience to perform their assigned tasks.	Adobe complies with accepted standards and IT best practices, as assessed through SOC 2 Type 2 reporting. Processes are in place for professional development and training to ensure that individuals responsible for the development and support of Adobe systems are qualified to perform their assigned tasks.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process for employee training and the management of training records. • Implementing a process to govern the use of Adobe Sign and ensuring that adequate training is given to users (Sender, Signer) prior to using the system for the application of electronic signatures. • Implementing a process to govern the administration of Adobe Sign and ensuring that adequate training is given to users (Account/Group Administrators) prior to performing administrative activities in the system. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.
Subsection 11.10 (j)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	The customer is responsible for demonstrating compliance to this regulation.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process to govern the application of electronic signatures, including measures designed to hold individuals accountable and responsible for actions initiated under or authorized by their electronic signatures.
Subsection 11.10 (k)(l)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Use of appropriate controls over systems documentation including: **(1)** Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	Adobe complies with accepted standards and IT best practices, as assessed through SOC 2 Type 2 reporting and ISO 27001 certification. Processes are in place to ensure that access to Adobe system design documentation is controlled.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process to govern the management of controlled documentation, ensuring that users have access to the correct and updated versions of standard operating and maintenance procedures (while limiting the distribution of highly sensitive documentation). • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

Subsection 11.10 (k)(2)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Use of appropriate controls over systems documentation including: **(2)** Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Adobe complies with accepted standards and IT best practices, as assessed through SOC 2 Type 2 reporting and ISO 27001 certification. Processes are in place for change management and to ensure the Product teams at Adobe create and update system design documentation as the product evolves.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process to manage changes to systems documentation (including operating procedures, specifications and configuration). • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

11.30 Controls for Open Systems.		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	All Adobe Sign documents (electronic records) are encrypted using PCI DSS approved encryption algorithms and stored securely within the data layer (databases and file store) managed by Adobe. Adobe Sign encrypts documents and assets at rest with AES 256-bit encryption and uses HTTPS TLS v1.2 to protect data in transit. Digital signatures are applied using public key infrastructure (PKI). The use of digital certificates issued by a trust service provider ensures authenticity of the signature and integrity of the record. Signed records and the associated audit reports may be extracted (downloaded) from the Adobe Sign service as PDF files which are certified by Adobe Sign using public key infrastructure (PKI). This provides assurance that the content of the record, including the signature, has not been tampered with since the certificate was applied. Access to signed electronic records provided through Adobe Sign can be restricted by placing a password on the document. Any copy of the document is encrypted and cannot be viewed until the password is supplied. Passwords must be communicated via a different communication system (e.g. mobile phone) to all relevant parties before they can open the document. These passwords are embedded into the PDF and are separate from the passwords used to log into Adobe Sign. Adobe Sign cannot recover or reset document passwords.	The use of password protection of records is based on a business decision depending on the sensitivity of the documents being signed using Adobe Sign. If deemed necessary, an organization using Adobe Sign as part of a regulated process is responsible for: • Determining whether the records should be password protected. • Defining the process governing the password protection of records.

11.50 Signature manifestations

Subsection 11.50 (a)

What the law requires	How Adobe Sign complies	Customer Responsibilities
Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: **(1)** The printed name of the signer; **(2)** The date and time when the signature was executed; and **(3)** The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Adobe Sign can be configured to display all the required components of the signature manifestation, including: 1) The printed name of the signer. For Internal signers, the system can be configured to prevent editing of the name by the Signer, so that the signature manifestation displays the printed name of the Signer as automatically derived from their user profile (if electronically signing) or from their Digital ID (if digitally signing). The user profile ties the individual's first and last name to a valid email address. For External Signers, the full name of the Signer will either be obtained from the user's existing ID with Adobe or must be entered at the time of signing. 2) The date and time when the signature was executed (including with time zone reference). The time stamp in the signature manifestation is applied when the Signer presses the Click to Sign button. 3) The meaning associated with the signature. Adobe Sign can be configured to allow signers to provide a custom (free-text) reason and/or to choose from a pre-determined list of signing reasons.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process to govern the application of electronic signatures, including provisions requiring users to specify the reason for signature. • Configuring the system in a manner allowing for the required components of the signature manifestation to be displayed.

Subsection 11.50 (b)

What the law requires	How Adobe Sign complies	Customer Responsibilities
The items identified [11.50 (a)] shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	The components of the signature manifestation are presented in the signed record (PDF). Moreover, when using digital signature functionality, the components of the signature manifestation are also included in the audit report. The components of the signature manifestation are human readable on the electronic display and any paper printout of the signed PDF.	Compliance to this regulation is achieved via Adobe Sign technical controls.

11.70 Signature/record linking

What the law requires	How Adobe Sign complies	Customer Responsibilities
Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	Once the final electronic signature is applied to a document, the electronic record is certified by Adobe Sign using public key infrastructure (PKI). This provides assurance that the record originated in Adobe Sign and that the content of the record, including the signature, has not been tampered with since the certification was applied. Adobe Sign generates an audit report capturing the history of activities for each agreement. The audit report and the signed document are linked together through the Transaction ID of the agreement on the Adobe Sign server.	Compliance to this regulation is achieved via Adobe Sign technical controls.

Subpart C — Electronic Signatures

11.100 General Requirements

Subsection 11.100 (a)

What the law requires	How Adobe Sign complies	Customer Responsibilities
Each electronic signature shall be unique to one individual and not reused by, or reassigned to, anyone else.	When creating the user in the customer's Adobe Sign account, a unique email address must be associated to the user. The Adobe Sign application can only differentiate users by their unique email address. The user's email address can only be added to a single Adobe Sign account. External users are uniquely identified by their email address and, if using the Phone authentication method, their phone number and a system generated verification code. When using digital signatures, the use of PKI technologies ensures that the signature is unique to an individual who owns the digital certificate and cannot be reassigned to others.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process to govern the creation and deactivation of user accounts, including provisions to ensure that no two individuals are associated to the same email address.

Subsection 11.100 (b)

What the law requires	How Adobe Sign complies	Customer Responsibilities
Before an organization establishes, assigns, certifies, or otherwise sanctions the individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual	When using simple electronic signatures, the customer is responsible for demonstrating compliance to this regulation. When using certificate-based digital signatures, the identity verification of the individual signer is performed by means of a registration process which may be performed by a trust service provider selected by the customer or delegated to another registration authority.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process to verify the identity of an individual prior to use of any electronic signature solution. Additionally, a customer using Adobe Sign's digital signature functionality is responsible for performing the initial assessment and periodic re-evaluation of the chosen trust service provider to ensure identity verification is performed in a controlled manner.

Subsection 11.100 (c)

What the law requires
Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

Subsection 11.100 (c)(1)

What the law requires	How Adobe Sign complies	Customer Responsibilities
The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.	The customer is responsible for demonstrating compliance to this regulation.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Communicating to the FDA the organization's intent to use electronic signatures as the legally binding equivalent of traditional handwritten signatures.

Subsection 11.100 (c)(2)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	Message templates can be configured in the customer's Adobe Sign account. The message is included in the Please Sign email sent to the signers. The text of the message can be customized to inform recipients of the legally binding nature of the signature. It is also possible to configure Email Settings in the customer's Adobe Sign account, providing standardized text in the footer of each email generated from their account to inform recipients of the legally binding nature of the signature. The Explicit Consent feature can be enabled to require the recipient to affirm their agreement with the Adobe Terms of Use as well as the Consumer Disclosure by actively checking the related boxes to signify agreement. By default, Adobe Sign exposes links to standard Terms of Use and Consumer Disclosure that the recipient agrees to before entering any information on the document. The text of the Consumer Disclosure can be customized to include a message informing them of the legally binding nature of the signature. With explicit consent, the user's acceptance of the Terms of Use and Consumer Disclosure will be reflected in the audit report.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a communication plan to inform all persons who are permitted to sign electronically that their electronic signature is the legally binding equivalent of their handwritten signature. An attestation should be provided by all signers to acknowledge that they have read and understood this obligation.

11.200 Electronic signature components and controls.		
Subsection 11.200 (a)(1)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Electronic signatures that are not based upon biometrics shall: **(1)** Employ at least two distinct identification components such as an identification code and password.	Adobe Sign can be configured to require signers to provide valid credentials (according to the specified identity verification method) at the time of signing (Click to Sign). If using Federated ID, the corporate directory services can be used to authenticate Internal users. For external signers, the authentication method can be selected by the sender at the time of setting up the agreement. The following authentication methods are available for the sender to choose from and this is controlled through configuration: • Adobe Sign authentication (which will prompt the signer to provide an ID they have created with Adobe and a password) • Phone authentication (which will prompt the signer to provide an email address and verification code) (Although other authentications mechanisms are possible, they are typically not used for 21 CFR Part 11 implementations of Adobe Sign.) If using certificate-based digital signatures, the system will request additional credentials (e.g. personal identification number (PIN) or one-time password (OTP)) issued from a trust service provider at the time of signing.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Configuring the system in a manner that enforces the use of an identity verification method that employs at least two distinct identification components.

Subsection 11.200 (a)(1)(i), 11.200 (a)(1)(ii)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. **(ii)** When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	Adobe Sign can be configured to require signers to provide valid credentials (according to the specified identity verification method) at the time of signing (Click to Sign), independent of the number of signings executed during a continuous period of system access.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Configuring the system in a manner that enforces the use of an identity verification method that employs at least two distinct identification components at the time of each signing.

Subsection 11.200 (a)(2)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Electronic signatures that are not based upon biometrics shall: **(2)** Be used only by their genuine owners.	A licensed user will log into Adobe Sign using a verified email address and valid password. Adobe Sign can be configured to enforce the use of credentials issued from a trust service provider. When using digital signatures, the use of PKI technologies ensures that the signature is unique to the individual who owns the digital certificate and cannot be reassigned to others. The digital certificate is controlled by its genuine owner. In addition, the trust service provider ensures the identification codes and passwords adopted for multi-factor authentication are uniquely bound to their owners.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process to govern the creation and deactivation of user accounts, including provisions to ensure that no two individuals are associated to the same email address. The customer is responsible for ensuring the email address assigned to an individual is associated to its genuine owner. • Implementing measures to prohibit the sharing of credentials by users. Additionally, a customer using Adobe Sign's digital signature functionality is responsible for performing the initial assessment and periodic re-evaluation of the chosen trust service provider to ensure signature authenticity.

Subsection 11.200 (a)(3)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Electronic signatures that are not based upon biometrics shall: **(3)** Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	Adobe complies with accepted standards and industry best practices for security and privacy, as assessed through SOC 2 Type 2 reporting. Processes are in place to ensure that documents, data and personal information are protected.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing measures to prohibit the sharing of credentials by users. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

Subsection 11.200 (b)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Not applicable. While an optional biometric comparison can be enabled when Adobe Sign's Government ID authentication process, this method is typically not used for 21 CFR Part 11 implementations of Adobe Sign.	Not applicable.

11.300 Controls for identification codes/passwords.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

Subsection 11.300 (a)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Each internal user is uniquely identified in the system with their email address. The user's email address can only be added to a single Adobe Sign account. External users are uniquely identified by their email address and, if using the Phone authentication method, their phone number and a system generated verification code. Digital signatures are applied using Public Key Infrastructure. The PKI standards adopted for the issuance of digital certificates ensure that the necessary private and public key-pairs are unique. In addition, trust service providers ensure that identification codes and passwords adopted for multi-factor authentication are uniquely bound to their owners.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process to govern the creation and deactivation of user accounts, including provisions to ensure that no two individuals are associated to the same email address. • Implementing a process to ascertain the identity of External signers prior to assigning them signature requests and to provide guidelines to the sender for determining the appropriate mode of authentication. Additionally, a customer using Adobe Sign's digital signature functionality is responsible for performing the initial assessment and periodic re-evaluation of the chosen trust service provider to ensure that identification codes and passwords adopted for multi-factor authentication are uniquely bound to their owners.

Subsection 11.300 (b)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Ensuring that identification code and password issuances must be periodically checked, recalled, or revised (e.g., to cover such events as password aging).	A licensed user will log into Adobe Sign using a verified email address and valid password. If not using Federated ID, Adobe Sign allows users with administrative privileges to specify the frequency at which this password must be reset by Internal users. The password history policy as well as the conditions for password strength and complexity can also be configured for internal users. If using Federated ID, the corporate directory services can be used to manage password controls. For external users, the use of the Phone authentication method ensures that no two signing activities use the same combination of credentials, since a new verification code is generated by the system every time the user needs to be authenticated. Adobe Sign's digital signature functionality relies on PKI services provided by the trust service provider. The trust service provider is responsible for the issuance of the identification codes and passwords adopted for multi-factor authentication.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Defining policies that specify the frequency at which passwords must be reset to prevent password aging. • Implementing a process to periodically review user access, ensuring that the appropriate privileges are granted to active users. Additionally, a customer using Adobe Sign's digital signature functionality is responsible for selecting a trust service provider that periodically checks, recalls, or revises the identification codes and passwords adopted for multi-factor authentication, per the customer's requirements.
Subsection 11.300 (c)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	The customer is responsible for deactivating individuals within their organization's account and for initiating forced password resets. If using Federated ID, the corporate directory services can be used to manage password resets. When using certificate-based digital signatures, the Public Key Infrastructure ensures the ability to suspend or revoke a digital certificate whose activation data has been lost, stolen or otherwise compromised. Trust service providers may issue temporary or permanent replacements based on their operational procedures, especially when digital certificates are hosted as a service on behalf of the owners.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process to allow users to report incidents where there is the possibility that their electronic signature has been compromised. • Implementing a process to govern user account administration, including provisions to force a password reset or to revoke access when a user's credentials have been compromised. Additionally, a customer using Adobe Sign's digital signature functionality is responsible for performing the initial assessment and periodic re-evaluation of the chosen trust service provider to assess the provider's capacity to issue temporary or permanent digital certificate replacements.

Subsection 11.300 (d)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	Adobe complies with accepted standards and best practices for cyber-security, as assessed through SOC 2 Type 2 reporting and ISO 27001 certification. Processes are in place to continually monitor unusual or anomalous activity and to ensure Adobe system administrators are notified upon user account lockouts. Adobe has implemented an incident response, mitigation, and resolution program. Processes have been implemented for security monitoring for the prevention and early detection of security vulnerabilities and incidents. Each security incident is investigated and mitigated by Adobe's incident response team to minimize risk to customers. Confirmed incidents are assigned a severity level based on impact, damage, or disruption to customers. Adobe will notify customers of a confirmed Personal Data Breach in accordance with applicable law. Breach notification is addressed in the contractual terms between Adobe and the customer. If using Adobe ID or Enterprise ID, Adobe Sign allows users with administrative privileges to specify the frequency at which passwords must be reset by Internal users. Additionally, the system will temporarily lock a user account after the maximum number of incorrect password entry attempts is exceeded. If using Federated ID, the corporate directory services can be used to manage password and user account lockout policies for Internal users. Logs can be monitored to detect and report unusual or suspicious activity on user accounts. When using certificate-based digital signatures, which are applied using Public Key Infrastructure, the trust service providers employ standards that require them to monitor the access to their PKI to detect and prevent unauthorized use of their systems and provide security reports to users and auditors.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Configuring the system or the corporate directory services in a manner that manages password resets. • Defining monitoring procedures to ensure unusual or suspicious activity on user accounts are detected, reported, and escalated (by the customer and/or by Adobe). • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices. Additionally, a customer using Adobe Sign's digital signature functionality is responsible for performing the initial assessment and periodic re-evaluation of the chosen trust service provider to ensure detection and prevention of unauthorized use.

Subsection 11.300 (e)		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Initial and periodic testing of devices such as tokens or cards that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	A licensed user will log into Adobe Sign using a verified email address and valid password; neither of these credentials are generated by a device. Trust service providers may use devices to generate identification codes or passwords required for the application of digital signatures. Testing of such devices falls under the responsibilities of the trust service providers and the customer.	An organization using Adobe Sign's digital signature functionality as part of a GxP regulated process is responsible for: • Performing the initial assessment and periodic re-evaluation of the chosen trust service provide to ensure adequate testing processes are followed.

4.2 EudraLex Volume 4 Annex 11

EudraLex is the collection of rules and regulations governing medicinal products in the European Union (EU). Of the 10 volumes that constitute EudraLex, Volume 4 contains guidance for the interpretation of the principles and guidelines of Good Manufacturing Practices (GMP) for medicinal products for human and veterinary use. Volume 4 is supported by numerous Annexes, including Annex 11 which broadly addresses the use of computerised systems in GMP regulated activities.

Regulations (EU Volume 4 Annex 11)

Principle
This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities. The application should be validated; IT infrastructure qualified. Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.

General		
1. Risk Management		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.	Adobe complies with accepted standards and IT maintains industry security certifications, as assessed through SOC 2 Type 2 reporting and ISO 27001 certification. Processes are in place to ensure Adobe systems are adequately tested as part of the development lifecycle. Risk management is incorporated into processes surrounding the development and maintenance of Adobe Sign. An Audit Committee oversees Adobe's enterprise risk management processes. The Audit Committee is independent from Adobe Management. As part of its functions, the Audit Committee meets regularly with the Information Security team to review key metrics concerning information security management activities.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Documenting the assessment of risks related to patient safety, data integrity and product quality surrounding the use of Adobe Sign. • Defining and implementing the controls necessary to eliminate or mitigate the identified risks to an acceptable level.

2. Personnel		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	Adobe complies with accepted standards and IT best practices, as assessed through SOC 2 Type 2 reporting. Adobe employees are required to take periodic training relevant to their job role and geographic location in areas concerning data privacy, data protection, and trade compliance.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process for employee training and the management of training records. • Implementing a process to govern the use of Adobe Sign and ensuring that adequate training is given to users (Sender, Signer) prior to using the system for the application of electronic signatures. • Implementing a process to govern the administration of Adobe Sign and ensuring that adequate training is given to users (Account/Group Administrators) prior to performing administrative activities in the system. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

3. Suppliers and Service Providers		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
3.1. When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous. **3.2.** The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment. **3.3.** Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled. **3.4.** Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	Adobe Service Commitments describe Adobe's service availability and notification process for the Adobe Sign services. Adobe has contractual agreements in place with third party vendors who process or store Adobe data. The contracts identify responsibilities, information security terms, and service level agreements. Procedures are followed to periodically monitor and review activities for inconsistencies or non-conformance. Third parties to whom any services are outsourced must undergo tailored, multi-level evaluation (per Adobe's vendor security review program and third party assurance review). Adobe assesses and addresses risks related to third party vendors. All analysis and conclusions are documented and reviewed in accordance with Adobe's vendor security review process via a streamlined vendor management platform. The Adobe Trust Center provides a vast amount of resources describing security, privacy, and availability of Adobe products, systems, and data. security, privacy, and availability of our products, systems, and data. Adobe maintains a Common Control Framework (CCF) that is used to support the organization's compliance and risk management strategy. Adobe Sign is certified compliant with numerous certifications, standards, and regulations, such as ISO 27001, SOC 2 Type 2, and PCI DSS, which can support customers in their vendor assessment programs.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Following a vendor selection and assessment process which provides rationale to support the method or approach taken to qualify Adobe as a suitable vendor. This assessment may consist of a periodic review of available third party reports and certificates (e.g. SOC 2, ISO). • Ensuring that formal agreements are executed with Adobe, and that the roles and responsibilities of each party are clearly defined. • Reviewing documentation provided by Adobe to support system validation activities that verify fulfilment of user requirements. • Ensuring the vendor assessment process is documented and information is available to inspectors when requested.

Project Phase		
4. Validation		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
4.1. The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment. **4.2.** Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process. **4.3.** An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available. **4.4.** User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle. **4.5.** The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately. *continued...*	Adobe complies with accepted standards and IT best practices, as assessed through SOC 2 Type 2 reporting and ISO 27001 certification. Processes are in place to ensure Adobe systems are adequately tested as part of the development lifecycle. Risk management is incorporated into processes surrounding the development and maintenance of Adobe Sign. Test coverage includes common use cases, and testing must be completed successfully prior to releasing software updates. A Quality Certificate is produced for every major software release as an attestation that the release complies with Adobe's quality standard for software development. Processes are in place for change management and to ensure the Product teams at Adobe create and update system design documentation as the product evolves. Changes to the Adobe Sign services are planned and communicated by Adobe prior to implementation of the change. Critical contacts named for an Enterprise or Business customer account may receive pre-release communications by email on a quarterly basis, directing customers to the pre-release notes. The email communications are sent 60, 30, and 15 days before release and again on the day post release. Adobe maintains the Adobe Sign service in a secure and controlled state. Third parties to whom any infrastructure services are outsourced must undergo strict evaluation (per Adobe's vendor assessment program). Adobe Sign is not intended to be used as a critical GMP system but is configurable to connect and/or be compatible with other databases or systems that may be considered as such.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Defining their business process needs (intended use). User requirements should be documented and should consider the outcome of regulatory impact and risk assessments. • Performing validation activities (with documented evidence) to demonstrate the Adobe Sign is fit for the customer's intended use of the system and meets regulatory requirements. As applicable, validation activities should include verifications to ensure documents uploaded to and retrieved from Adobe Sign are not altered. Procedural controls should be implemented to define the validation approach in the context of GxP regulated activities. • Implementing procedural controls to govern the controlled operation of the system and how changes are made to the Adobe Sign account configuration. • Ensuring an up to date system description is maintained, describing how Adobe Sign is implemented by the customer. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

4. Validation *continued*		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system. **4.7.** Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy. **4.8**. If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.		

Operational Phase		
5. Data		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.	All Adobe Sign documents (electronic records) are encrypted using PCI DSS approved encryption algorithms and stored securely within the data layer (databases and file store) managed by Adobe, as described in the Adobe Sign Security Overview. Adobe Sign encrypts documents and assets at rest with AES 256-bit encryption and uses HTTPS TLS v1.2 to protect data in transit.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Establishing appropriate logical security policies and access controls to protect the integrity of records signed using Adobe Sign. • Ensuring (through validation activities) that the transfer of data to/from Adobe Sign does not impact data integrity. • Ensuring the security of electronic documents transferred to/from the Adobe Sign environment.

6. Accuracy Checks		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by riskmanagement.	If needed, compliance to this regulation is achieved through customer-implemented controls. Adobe does not enter customer data manually.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Establishing processes to identify critical data (e.g. data that influences a batch release decision, data that determines compliance with critical quality attributes) and to enforce the review of manually entered critical data, based on the business process requirements supported by the system.

7. Data Storage		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
7.1. Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. **7.2.** Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.	Adobe Sign is compliant with rigorous security standards and IT best practices, as assessed through SOC 2 Type 2 reporting and ISO 27001 certification. Processes have also been implemented to govern backup management and system monitoring. The signed record and its audit report are made available in PDF format and can be viewed with a PDF viewer. These PDFs are certified and sealed, providing proof of origin and integrity. All Adobe Sign documents (electronic records) are encrypted and stored securely within the data layer (databases and file store) managed by Adobe. Users with appropriate permissions can download a signed agreement and its audit report from Adobe Sign for retention in a system used by the customer to manage electronic records, e.g. Electronic Document Management System (EDMS). Customers can retrieve their data from the Adobe Sign services throughout the duration of their contract with Adobe, unless a Privacy Administrator deleted an agreement or data governance policies and retention rules are defined. Retention rules specify the timeframe after which transactions, agreements, and the supporting audit and personal data can be automatically deleted from Adobe Sign. During the customer's license term, the data will not be deleted until the customer takes action to delete the agreements explicitly. If no retention rules are defined, Adobe will retain all customer documents on the service for as long as the account is active. Adobe Service Commitments describe Adobe's service (data) availability and notification process for the Adobe Sign services.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Defining record retention policies and, as applicable, configuring the system in a manner that enforce retention rules. • Implementing data repatriation process(es) for moving signed records and the associated audit reports back to a customer-managed EDMS. The process for retrieval of records from the Adobe Sign service should include provisions to verify that these are certified by Adobe. • Implementing appropriate backup infrastructure and policies for records retrieved from the Adobe Sign service and retained in the customer-managed EDMS. The backups must be periodically tested. Archiving policies must be established to ensure availability of the data throughout the retention period. • Establishing appropriate Logical Security policies and access controls to protect the integrity of records signed in Adobe Sign. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

8. Printout		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
8.1. It should be possible to obtain clear printed copies of electronically stored data. **8.2.** For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	The signed record and its audit report are made available in PDF format. These can be viewed electronically with a PDF viewer and on any paper printout. These PDFs are certified and sealed, providing proof of origin and integrity. Refer to Annex 11, article 9 - Audit Trails for details of what gets captured on the audit report. Adobe Service Commitments describe Adobe's service availability, ensuring the data is accessible.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Establishing the process for using the Adobe Sign service for viewing or generating printed copies of signed records and the associated audit reports. • Physical security of printed records

9. Audit Trails		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.	Adobe Sign generates an audit trail capturing the history of activities for each agreement within the Adobe Sign service. This audit trail functionality cannot be disabled by the customer. The audit trail can be retrieved as an audit report in PDF format and can be viewed with a PDF viewer. The audit report is associated to the signed document and these are linked together through the Transaction ID of the agreement on the Adobe Sign server. The audit report and the associated signed document can be retrieved as two distinct PDF files or merged into a single PDF file. The PDF is certified with a digital certificate owned by Adobe, providing proof of origin and integrity of the audit trail and to prevent tampering. The audit report captures each signature event, including the identity (full name and email address) of the user who electronically signed the document. Actions recorded in the audit report are sequential and do not obscure previous audit trail entries. All entries are date and time-stamped using Adobe server time. The time stamp is applied when the Signer presses the Click to Sign button. The audit report also captures the identity of a user who decides to reject the document or cancel the signature process. An authorized user (sender) may upload a document in the Adobe Sign portal. If not already in PDF format, Adobe Sign will convert compatible file formats into PDF format prior to sending a document for signature. Once the agreement is in process (as of when the first recipient completed their signature), the document in PDF format cannot be modified. As a result, actions that modify electronic records are not presented in the audit report. Retention rules can be configured to define the timeframe after which transactions, agreements, and the supporting audit and personal data can be automatically deleted from the Adobe Sign service. When creating a retention rule, it is possible to define a distinct retention period for the associated audit trail. If this option is not enabled, the audit record will not be deleted.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing data repatriation process(es) for moving signed records and the associated audit reports back to a customer-managed EDMS. The process for retrieval of records from the Adobe Sign service should include provisions to verify that these are certified by Adobe. • Defining a process and the frequency for reviewing audit trail data.

10. Configuration and Change Management		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	Adobe complies with accepted standards and IT best practices, as assessed through SOC 2 Type 2 reporting and ISO 27001 certification. Processes are in place for change management and to ensure the Product teams at Adobe create and update system design documentation as the product evolves. Changes to the Adobe Sign service are planned and communicated by Adobe prior to implementation of the change.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process to monitor and assess the impact of changes announced by Adobe. • Implementing a process to manage any configuration changes to the Adobe Sign account settings triggered by a user request. • Documenting the process and relevant changes made to systems connected to or entirely separate from a customer's Adobe Sign instance.
11. Periodic Evaluation		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	Adobe complies with accepted standards and IT best practices, as assessed through SOC 2 Type 2 reporting and ISO 27001 certification. Product teams at Adobe create and update system design documentation as the product evolves. Processes have been implemented for information security monitoring. Security monitoring alert criteria, security hardening and baseline configurations, vulnerability assessment scan tools, and data classification criteria are periodically reviewed and updated. Third party vendor assurance reports are reviewed on a periodic basis. If control gaps are identified, remediation actions are implemented to address the impact of the disclosed gaps. Adobe publishes release notes outlining the history of changes and improvements made to the Adobe Sign service and features.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process to govern the periodic review of the state of the Adobe Sign account, its configuration, and related systems documentation.

12. Security		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
12.1. Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. **12.2.** The extent of security controls depends on the criticality of the computerised system. **12.3.** Creation, change, and cancellation of access authorisations should be recorded. **12.4.** Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	User entitlement can be managed from within the Adobe Sign account or through the Adobe Admin Console. Adobe Sign uses a role-based model to control authorization and system access. Users with administrative privileges can add individuals as Adobe Sign users to the customer's account and can assign roles (Signer, Sender) to grant signing and sending authority to select individuals within their account. Only administrators can access the areas of the system where account administration and configuration activities are performed. Adobe Sign can be configured to require signers to authenticate at various moments (including upon system login, upon opening an agreement to view the document, and when applying a signature). Configuration settings and user permissions provide safeguards against unauthorized access to documents. Multi-factor authentication methods can be used to verify the signer's identity. The customer's Adobe Sign account can be configured to mandate the use of a specific method to verify the signer's identity. Different authentication controls can be configured to accommodate Internal and External recipients. Adobe provides online content and support for configuring security settings in the customer's account. Adobe complies with accepted standards and IT best practices, as assessed through SOC 2 Type 2 reporting and ISO 27001 certification. Processes are in place to ensure physical and logical security measures are implemented. Adobe captures and manages system logs in order to help protect against unauthorized access and modification. Adobe Sign encrypts documents and assets at rest with AES 256-bit encryption and uses HTTPS TLS v1.2 to protect data in transit.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process for user access management, including clear criteria for granting/revoking user access and how access requests are documented. • Configuring the system in a manner that enforces user authentication to restrict system access. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and best practices regarding logical and physical security. • Ensuring the accuracy of recipient information. • Ensuring the security of overall customer network and third party systems connected to the Sign services.

13. Incident Management		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	Adobe has implemented an incident response, mitigation, and resolution program. Processes have been implemented for security monitoring for the prevention and early detection of security vulnerabilities and incidents. Each security incident is investigated and mitigated by Adobe's incident response team to minimize risk to customers. Confirmed incidents are assigned a severity level based on impact, damage, or disruption to customers. Adobe will notify customers of a confirmed Personal Data Breach in accordance with applicable law and relevant contractual terms between Adobe and the customer.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process for reporting, investigating, and resolving incidents for all systems, networks, and platforms within the customer's scope of responsibility and control. • Notifying Adobe immediately of any security incident which may impact the security of a customer's Sign account or introduce vulnerabilities that could threaten the security, availability or integrity of Sign services known to or reasonably suspected by customer.

14. Electronic Signature		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Electronic records may be signed electronically. Electronic signatures are expected to: **a)** have the same impact as hand-written signatures within the boundaries of the company, **b)** be permanently linked to their respective record, **c)** include the time and date that they were applied.	Adobe Sign can be configured to display the following information in the signature manifestation: • The printed name of the signer • The date and time when the signature was executed (including with time zone reference) • The meaning associated with the signature. Sign users may manually sign agreements with wet signatures, import an image of their wet signature, sign a document manually using a touch or e-pen enabled screen, or customize a typed version of their signed name. The availability of these options depends on the underlying document settings (to reflect applicable legal or other preferences or requirements), and the preferences of and specific hardware features available to signatories. Once the final electronic signature is applied to a document, the electronic record is certified by Adobe Sign using public key infrastructure (PKI). This provides assurance that the content of the record, including the signature, has not been tampered with since the certificate was applied.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing a process to govern the application of electronic signatures, including measures designed to hold individuals accountable and responsible for actions initiated under or authorized by their electronic signatures.

15. Batch Release		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.	If needed, compliance to this regulation is achieved through customer-implemented controls.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Defining procedures to control the use of the system for certifying and releasing batches and clarifying the role or Qualified Persons in this process.

16. Business Continuity		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	Adobe complies with industry best practices and deploys a comprehensive, ISO 22301-certified program for Business Continuity and Disaster Recovery. Processes are in place to ensure the Adobe Corporate Business Continuity Plan is tested on an annual basis and results are documented. Adobe Sign's hosting environment is designed to withstand service disruptions. Multiple cloud providers are used and multiple geographically dispersed cloud regions are leveraged to provide failover capability. Processes are in place to ensure the cross-region failover and failback capability is tested. As part of Adobe's Business Continuity and Disaster Recovery (BCDR) program, disaster recovery testing for Adobe Sign is conducted on an annual basis and results are documented. Adobe Service Commitments describe Adobe's service (data) availability and notification process for the Adobe Sign services. The availability status of the Adobe Sign service is shared on the Adobe cloud status page.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and best practices regarding business continuity. • Ensuring that mechanisms for Disaster Recovery and Business Continuity are in place and tested, should any problem arise with Adobe Sign. Consideration should be given to data repatriation process(es) for moving signed records and the associated audit reports back to customer-managed systems and the availability of adequate backup infrastructure and policies to ensure this data remains available. Manual or alternative e-signature signature processes should be in place in the event of an extended outage and storage of critical documents should be backed up in secure systems designed for this purpose.

17. Archiving		
What the law requires	**How Adobe Sign complies**	**Customer Responsibilities**
Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.	All Adobe Sign documents (electronic records) are encrypted and stored securely within the data layer (databases and file store) managed by Adobe. By default, all documents are retained on the Adobe Sign service for as long as the customer's account is active. For customers who want to delete the original documents from the Adobe Sign service, the account administrator can set up data governance policies for their account. Retention rules can be defined to specify the timeframe after which transactions, agreements, and the supporting audit and personal data can be deleted. If no retention rules are defined, Adobe will retain all customer documents on the service for as long as the account is active. During the customer's license term, the data will not be deleted until the customer takes action to delete the agreements explicitly. If a retention rule was defined by the customer, the agreements will be deleted automatically after the specified timeframe.	An organization using Adobe Sign as part of a GxP regulated process is responsible for: • Implementing data repatriation process(es) for moving signed records and the associated audit reports back to a customer-managed EDMS. • Implementing appropriate backup infrastructure and policies for records retrieved from the Adobe Sign service and retained in the customer-managed EDMS. The backups must be periodically tested. Archiving policies must be established to ensure availability of the data throughout the retention period.

5 Contact Info

To learn more about how Adobe Sign can benefit your organization, contact your Adobe sales representative today at 1-800-87ADOBE.

This document was prepared through a collaboration between Adobe and Montrium Inc. Learn about Montrium at www.montrium.com.

6 Disclaimer

This document is intended to help businesses analyze their responsibilities relating to 21 CFR Part 11 and Annex 11 Compliance. Adobe does not provide legal advice on any specific use cases, and this analysis is not meant to provide any specific legal guidance. To apply this analysis to any specific use case needs, please consult an attorney. To the maximum extent permitted by law, Adobe provides this material on an "as-is" basis. Adobe disclaims and makes no representation or warranty of any kind with respect to this material, express, implied or statutory, including representations, guarantees or warranties of merchantability, fitness for a particular purpose, or accuracy