WHITE PAPER

Adobe® Vendor Security Review Program

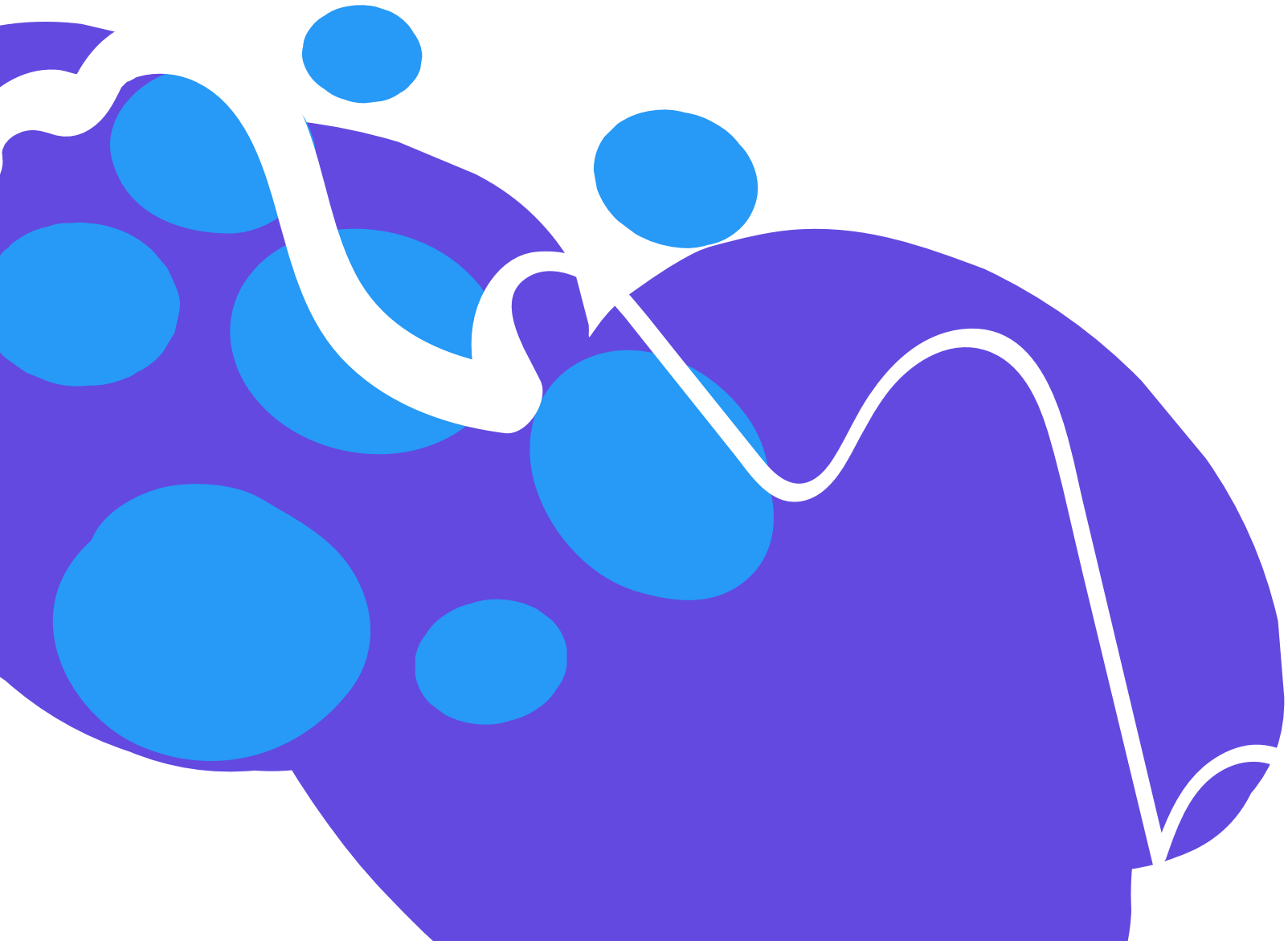


Table of Contents

Overview

Managed by the Adobe Security team, Adobe's Vendor Security Review (VSR) program includes a set of requirements to which third-party vendors that collect, store, process, transmit, or dispose of Adobe Restricted, Confidential, or Internal data outside of Adobe-controlled physical offices or data center locations must adhere. Typical scenarios include vendors processing and storing Adobe data at their site, within cloud services (e.g., SaaS, PaaS, IaaS, and XaaS), and in data centers.

The Adobe VSR program evaluates each vendor's compliance with the Adobe Vendor Information Security Standard, providing a risk-based review of the vendor's security practices and enabling Adobe managers to make fact-based decisions concerning whether or not to enter into a relationship with that vendor.

The management of vendor relationships and their interactions with Adobe information and technology resources is an essential element of information security. The VSR program is a logical extension of Adobe's belief that every action taken on or interaction with data should be conducted with a lens of security to help ensure the security, privacy, and availability of our customers' and employees' data, no matter where it is stored or processed, which is one of the key controls within the Adobe Common Controls Framework (CCF). With the VSR program, Adobe helps ensure that its culture of security extends to any vendor with whom the company does business.

Adobe Vendor Security Review Program Process

Business owners within Adobe that wish to engage with a third-party vendor initiate the process with a VSR request, which includes a description of the service provided by the vendor, whether the vendor will process Adobe data off-site, and the classification of the data the vendor intends to process.

Based on the information provided by the business owner, Adobe sends the main point of contact at the vendor a detailed questionnaire, including questions from each security control area (see the VSR Security Controls section below).

After the vendor completes and returns the questionnaire, Adobe Security analysts review the information and perform a gap assessment. A vendor is assigned a risk level score of "critical," "high," "medium," or "low" based upon a risk matrix used by our risk analysts. If Adobe finds any gaps in or deviations from Adobe security standards, a risk analyst discusses the gaps and suggests potential remediations with the business owner. The analyst then documents the recommended remediation and the actions to be performed by the vendor and/or the business owner.

Data Classification

Adobe developed the Adobe Data Classification and Handling Standard to aid in ensuring the security and privacy of all data that Adobe collects, processes, stores, uses, or otherwise handles, regardless of whether the data is owned by Adobe or a third party, where the data is located (e.g., Adobe data center or colocation), or the type of hardware or media on which the data resides, whether paper or electronic (e.g., server, desktop, laptop, mobile device, USB flash drive).

The Adobe Data Classification and Handling Standard establishes that all data collected, processed, transmitted, stored, or destroyed by or on behalf of Adobe must be classified and protected in accordance with its designated classification. The specific classifications in the standard define with whom employees can share Adobe data and determine where and how to share, protect, and secure this data.

The Adobe Data Classification and Handling Standard includes four (4) classifications:

- Adobe Restricted
- Adobe Confidential
- Adobe Internal
- Public

A VSR is required for all third-party vendors that store or process data classified as Adobe Restricted, Adobe Confidential, or Adobe Internal off premises (not at Adobe). Depending on the classification of the data handled by the vendor and the risk level assigned by our risk analysts, Adobe reassesess vendor controls every one to three years (see the Vendor Recertification section below).

Each data classification includes specific protection and handling requirements, and if data falls into multiple classifications, it must be protected in accordance with the most restrictive classification.

Any business owner requesting an exception to the Adobe Data Classification and Handling Standard must submit a written request to the appropriate management personnel for review and approval.

If Adobe finds that data that should be classified as Adobe Restricted or Adobe Confidential has been handled incorrectly, either due to incorrect classification or negligence in its handling, Adobe may take disciplinary action against the offender.

Adobe Restricted Data

Adobe Restricted data is the most restrictive classification and requires the most care; Only very limited segments of the Adobe workforce need access to Adobe Restricted data to perform their jobs. Unauthorized disclosure of Adobe Restricted data could cause severe harm to Adobe, its employees, customers, stockholders, and business partners. Adobe Restricted data includes *only* the following:

- Cardholder data, as defined by the PCI DSS
- Bank account numbers
- Social Security and taxpayer identification numbers relating to an individual
- Driver's license numbers or identification card numbers used to verify an individual's identity (e.g., state, military, student, voter, tribal, operator's number)
- Passport information
- Any system that stores or manages credentials on behalf of other systems or users, including (without limitation) Adobe Identity Management Services (IMS), Active Directory, Vault and CyberArk, but not personal password managers.
- Credentials, secrets, tokens, and private keys of any kind and other keys permitting access to systems if they grant access to Adobe Restricted data processed or stored by that system. A system that only processes or stores Adobe Confidential data will generally not need to treat its credentials as Adobe Restricted data.
- Digital certificates used for signing Adobe software
- Medical or health information, including electronically protected health information (ePHI)
- Federal classified or intelligence contracts
- Security question response (including mother's maiden name) or Personal Identification Number (PIN)
- Private key digital signatures
- Biometric information
- Genetic information
- Racial origin
- Ethnic origin
- Political opinions
- Religious beliefs

- Philosophical beliefs
- Trade union membership
- Sex-life information
- Sexual orientation
- Criminal offenses and convictions
- Birth certificate
- Date of birth (day, month, and year) in combination with full name
- Marriage certificate
- Information or data collected through use or operation of an automated license plate recognition system

Classification	Examples	Impact of Unauthorized Disclosure
Adobe Restricted data has a High Business Impact	Regulatory protected data, material financial data, intellectual property, passwords, and credentials	Likely to cause severe harm to Adobe, its employees, customers, stockholders, or business partners
Adobe Confidential data has a Medium Business Impact	People-related data (e.g., salary, benefits); data with need-to-know restrictions, such as source code, customer files, product roadmaps; and Adobe financial information	Likely to cause significant harm to Adobe, its employees, customers, stockholders, or business partners
Adobe Internal data has a Moderate Business Impact *Note: The default type for unclassified data is Internal*	Operational planning, collaboration and internal communications, and Adobe IT Knowledge Center articles	May cause minor embarrassment or operational inconvenience to Adobe
Public data	Information that is openly available	No impact

Adobe Confidential Data

Only limited segments of the Adobe workforce require access to data classified as **Adobe Confidential** in order to perform their jobs. Unauthorized disclosure of Adobe Confidential data would likely cause significant harm (e.g., financial, contractual, or legal or reputational damage or service disruptions) to Adobe, its employees, customers, stockholders, and business partners.

Adobe Confidential data includes:

- Data that Adobe is contractually required to treat as confidential
- Personal information (PI) about an individual, including free users, paid users, enterprise users, suppliers, or employees.* This can include directly identifiable personal information, such as name, email address, phone number, home address, gender, or precise geolocation information. Personal information can also include indirectly identifiable information about or relating to an individual, such as a user GUID, IP address, cookie ID, or device identifier.
- Content or data that customers, partners, or users provide to Adobe and that Adobe is under an agreement or regulation to protect*
- Source code managed or maintained by Adobe unless it is outbound open source code, approved for release by Adobe in accordance with the Open Sourcing Adobe Technology guidelines.
- Documents such as, but not limited to, technical architecture documents, system descriptions, operational procedures, planning and testing (such as for disaster recovery or incident response), change management, software development lifecycle (SDLC) docs, and product roadmaps.
- Adobe product serial numbers
- Non-public Adobe product or service security vulnerabilities

Adobe Internal Data

Adobe Internal is data that large segments of the Adobe workforce access to perform their jobs or facilitate their work experience and is intended for use only within Adobe. Examples of Adobe Internal data include, but are not limited to:

- Information on company intranet (*"Inside Adobe"*)
- Adobe IT Knowledge Center articles
- Adobe directory information
- Adobe corporate policies and standards

* Unless the personal information meets the definition of Adobe Restricted data

Public Data

Public data is data that Adobe intentionally shares with the general public. There are no protection or handling requirements for Public data. Examples of Public data include:

- Information available on Adobe.com that does not require login
- Open source software, open source code, or software development kits (SDKs), unless contractually required to label as a higher classification
- Publicly distributed marketing materials
- Publicly available regulatory filings
- Data that Adobe customers intend to be public

VSR Security Controls

The VSR program assesses the following security controls for every third-party vendor that stores or processes Adobe Restricted, Confidential, or Internal data outside of Adobe-controlled physical offices or data center locations:

- **Assertion of Security Practices** — Review of security certification attestation reports (SOC 2 Type II, ISO 27001) and internal security policies and standards
- **User Authentication** — Password policies, access control processes, and support of multi-factor authentication (MFA)
- **Logging and Auditing** — Details about system/application/network logs and retention periods
- **Data Center Security** — Physical security controls in locations where Adobe data is hosted
- **Vulnerability and Patch Management** — Cadence of external/internal vulnerability assessments and penetration tests as well as timelines for vulnerability remediations
- **Endpoint Protection** — Policies that cover endpoint security
- **Data Encryption** — Encryption of data at rest and in transit
- **Data Backup and Recovery** — Frequency of backups, encryption, testing, and existence of a disaster recovery (DR) plan
- **Breach Notification** — Compliance with Adobe's breach notification requirement
- **Service Provider Access** — Policies that address the security of third-party providers
- **Application Security** — Secure coding practices

- **Network Security** — Security controls in the network layer, including segmentation and firewalls
- **Service Decommissioning** — Data destruction after service termination
- **PCI Compliance** — How and where vendors process credit card information
- **User-generated Content** — Ensure uploads are virus- and malware-free

The Adobe Vendor Information Security Standard

The Adobe Vendor Information Security Standard establishes the responsibilities and security requirements regarding vendor engagements and applies to all vendors that collect, store, process, transmit, or dispose of data. The standard simplifies and streamlines the process of vendor compliance with Adobe's information security requirements.

Some requirements in the standard apply only to those vendors that handle specific classifications of data, described in the Data Classificiation section above, for which Adobe has unique obligations (e.g., cardholder data or ePHI). Any vendor handling such data must comply with all generally applicable requirements and any additional requirements specified for such data. Adobe also requires vendors to adhere to best practices regarding application security including avoiding the OWASP Top 10 vulnerabilities and security training for their employees.

Vendor Engagement

All vendor engagements must be reviewed and approved by Adobe's procurement, information security, and legal teams prior to allowing any third party to collect, access, store, process, transmit, or dispose of Adobe Restricted, Confidential, or Internal data, as defined in the Data Classification section above.

Vendor Onboarding

Adobe's vendor onboarding process includes steps to classify the information that will be handled by each individual vendor. The Adobe business owner who wants to onboard a new third-party vendor must accurately complete the data classification section of a vendor onboarding request to reflect the specific data that the vendor will process or store on Adobe's behalf.

To ensure ongoing compliance with the Adobe Vendor Information Security Standard, all third-party vendors must sign a security addendum as part of the contract negotiations during the onboarding process. Terms are reviewed annually, at contract renewal.

As Adobe contractors, all third-party vendors must adhere to the Adobe Bring Your Own Device (BYOD) Standard. This standard applies to any device owned by the third-party vendor or its employees capable of connecting to the Adobe network. When conducting Adobe business on a BYOD, third-party vendors and their employees must comply with all applicable laws and regulations as well as Adobe's policies, where their role is applicable. To maintain security of Adobe Restricted, Adobe Confidential, and all Personal Information (regardless of classification) data, individuals utilizing a BYOD must ensure that all such data is accessed from and saved to a trusted Adobe-owned data store (e.g., SharePoint or OneDrive) and not on the BYOD. All third-party connections are audited on a periodic basis to ensure compliance.

Adobe also helps ensure its cloud service providers meet the Adobe Vendor Information Security Standard through an annual review of controls using their SOC 2 Type II reports and other certifications.

Vendor Deficiencies

Vendors assessed as "Low Risk" by the VSR process immediately proceed through the rest of the vendor onboarding process. If the VSR is completed as part of a recertification, the vendor remains on the approved vendor list.

Vendors assessed as "Medium Risk," "High Risk," or "Critical Risk" by the VSR process are required to take steps to ensure that risk is either mitigated or explicitly accepted by Adobe management. Once this plan has been agreed to and signed by Adobe management, the vendor is approved to proceed through the vendor onboarding process. If the Adobe business or relationship owner agrees to actions that mitigate risk, that manager must ensure that the vendor follows the risk mitigation steps according to Adobe's documented commitments.

Vendor Recertification

Vendors that store or process Adobe Restricted data off-site must complete a security review annually, while vendors handling Adobe Confidential or Adobe Internal data are reassessed every one to three years, depending on the risk level assigned by Adobe risk analysts. As part of the recertification process, Adobe reviews the vendor's data classification, security controls, changes to infrastructure or application since last review, gaps or remediations since last review, and updates the risk assessment.

Vendors and owners handling Adobe Restricted or Adobe Confidential data must update their security assessment every one to three years. Adobe will conduct a security review if the vendor replies with any high-risk responses.

If the existing data classification for a particular set of data is brought into question prior to the required review cadence (e.g., product change, audit, or other inquiry), a classification review must be completed.

Privacy Assessment

A privacy assessment is an integral part of the vendor onboarding process. If a vendor will be processing any Personal Information on behalf of Adobe, they will need to complete not only the VSR, but also a privacy questionnaire. The Adobe Privacy team reviews the privacy questionnaire and the data classification section to determine if there are any privacy issues that need attention and whether any privacy and security terms (described in the following section) are required.

Legal Obligations

Data Processing Agreement

Adobe requires any vendor processing Adobe Restricted, Adobe Confidential, or Personal Information (regardless of classification) on our behalf to sign a data processing agreement (DPA), which is a written contract between Adobe and the vendor that governs the following actions:

- Processing — Documents both parties' data protection obligations as it pertains to accessing, collecting, processing, transmitting, sharing, and storing PI data.
- Transferring — Documents the cross-border data transfer requirements, where applicable, within the scope of services as described in the Master Agreement.
- Securing — Documents the technical and organizational controls to be implemented and maintained by vendor.

Upon signing the DPA, the vendor must adhere to all requirements stated in the document, which are detailed below.

Elements of the Adobe DPA

- **Security** — Contains provisions that describe the minimum security requirements with which a vendor must comply when handling Adobe information, including when and how a vendor must notify Adobe of a security incident involving access controls, security assessments, logging requirements, and processing data subject requests.
- **Privacy** — Documents both Adobe's and the vendor's obligations under applicable data protection laws, including GDPR. More specifically, the DPA addresses:

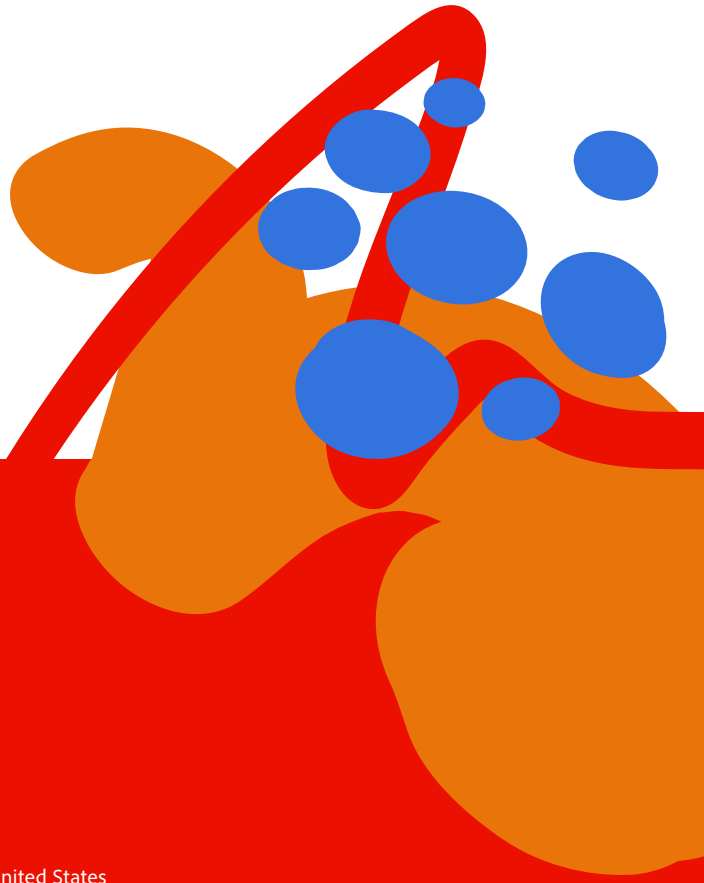
- Processing — A vendor may only process or store Personal Information to the extent necessary to perform its obligations under the Master Agreement, as per written instructions from Adobe and in compliance with all applicable laws.
- Transfer — A vendor accessing or storing any Personal Information from outside the originating country (i.e., cross-border transfer) may be required to have a data transfer mechanism, depending on the country of origin.

Ethical Behavior

Adobe expects its vendors to adhere to its business code of conduct which ensures strong anti-corruption and anti-bribery best practices. Vendors' codes of conduct are reviewed as part of the onboarding process to ensure they meet Adobe's published code of conduct standards.

Conclusion

The Adobe Vendor Security Review program is a critical element in helping ensure that third-party vendors with whom we do business adhere to the same stringent information security standards as Adobe itself. By requiring vendors to comply with the Adobe Vendor Information Security Standard, Adobe business owners can make informed decisions about relationships with third parties that collect, store, process, transmit, or dispose of Adobe Restricted, Confidential, or Internal data outside of Adobe-controlled physical offices or data center locations.



Adobe

8/22