Adobe® Vendor Risk Assessment Program

Overview

Managed by the Adobe Information Security team, Adobe's vendor risk assessment program — called "Guardrails" — is a set of requirements to which third-party vendors that collect, store, process, transmit, or dispose of Adobe Internal, Confidential, or Restricted 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, cloud services (e.g., SaaS, PaaS, IaaS, and XaaS), LAN-to-LAN VPN connections, and data centers.

The Guardrails Risk Assessment program evaluates each vendor's compliance to Adobe's 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. Guardrails 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 Guardrails program, Adobe helps ensure that its culture of security extends to any vendor with whom the company does business.

Table of Contents

Adobe Guardrails Risk Assessment Program Process

The Guardrails Risk Assessment (GRA) program evaluates a third-party vendor's compliance with the Adobe Vendor Information Security Standard (described above).

Business owners within Adobe that wish to enter into a relationship with a third-party vendor initiate the process with a GRA 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 GRA Security Controls section).

After the vendor completes and returns the questionnaire, Adobe information security analysts review the information and perform a gap assessment. A vendor is assigned a risk level score of "high," "medium," "low," or "critical" 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 holds discussions with the business owner to understand the details about the gap and to provide potential remediation suggestions. The analyst 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, 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 thumb drive). The standard establishes that all data collected, processed, transmitted, stored, or destroyed by or on behalf of Adobe must be classified and then 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 GRA is required for all third-party vendors that store or process data classified as Adobe Restricted, Confidential, or Internal off-premise (not at Adobe). Depending on the classification of the data handled by the vendor, a new GRA is required either annually or bi-annually (see Recertification section).

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 vendor requesting an exception to the Data Classification and Handling Standard must submit a request in writing 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, or business partners. Adobe Restricted data includes 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 number used to verify an individual's identity (state, military, student, voter, tribal, operator's number, etc.)
- Passport information
- Credential stores used to authenticate Adobe users or employees, such as the Renga system and Active Directory (but not including personal password managers, such as Splash ID)
- Credentials, secrets, tokens, or keys permitting access to systems storing Restricted data or permitting decryption of Restricted data (e.g., identity management systems, deployment systems, or secret stores)
- 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
- Marriage certificate
- Information or data collected through use or operation of an automated license plate recognition system

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

Adobe Confidential Data

Only limited segments of the Adobe workforce need access to data classified as Adobe Confidential in order to perform their jobs. Unauthorized disclosure of Adobe Confidential data would likely cause significant harm (such as financial, contractual, or legal or reputational harm 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) (unless the personal information meets the definition of Adobe Restricted data below) 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, or precise geolocation information. Personal information can also include indirectly identifiable personal information, such as a user GUID, IP address, cookie ID, or device identifier.

- Content or data that customers, partners, or users provide to Adobe (unless the content or data meets the definition of Restricted data below)
- Adobe source code (proprietary not "open source")
- Documents such as technical architecture documents, system descriptions, operational procedures, planning and testing (such as for disaster recovery or incident response), change management, SDLC docs, and product roadmaps
- Non-public Adobe product or service security vulnerabilities
- Employee gender

Adobe Internal Data

Adobe Internal data is data large segments of the Adobe workforce access to perform their jobs or facilitate their work experience. Internal data is intended for use only within Adobe. Examples of Adobe Internal data include:

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

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

GRA Security Controls

The GRA 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
- **Logging and Audit** — Details about system/app/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 pen tests as well as timelines for vulnerability remediations
- **End-point protection** — Policies that cover end-point security
- **Data Encryption** — Encryption of data in rest and transit
- **Data Backup and Recovery** — Frequency of backups, encryption, testing, and existence of a 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, firewalls, et
- **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 governance requirements regarding vendor information security 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 to 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 Classification section above) for which Adobe has unique obligations (e.g., cardholder data or electronically protected health information). 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 and Handling Standard described 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 Guardrails risk assessment 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 that is 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, all individuals utilizing a BYOD must ensure that Adobe Restricted, Adobe Confidential, and PI (regardless of classification) data is not stored or transmitted on a BYOD. Rather, all data must be accessed and saved from a trusted Adobe-owned data store (e.g., SharePoint or OneDrive). All third-party connections are audited on a periodic basis to ensure compliance.

Adobe also helps ensure AWS and Azure 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 GRA process immediately proceed through the rest of the vendor onboarding process. If the GRA is done 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 GRA 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 or Adobe Confidential data off-site must undergo and obtain recertification annually, while vendors handling Adobe Internal data are re-certified every two years. Adobe reviews the third-party vendor's data classification, security controls, changes to infrastructure or application since last review, gaps, or remediations since last review and documents the updated risk assessment.

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.

Vendors and owners handling Adobe Restricted or Adobe Confidential data must recertify the handling (i.e., security) of Adobe data annually or biennially depending on the risk level. Adobe Internal data is recertified biennially, regardless of risk level.

Privacy Assessment

A privacy assessment is an integral part of the Guardrails process. If a vendor will be receiving any Restricted, Confidential, or Personal Information from Adobe, they will need to complete not only the Guardrails assessment (GRA), but also a privacy questionnaire addendum. The Privacy team reviews the privacy questionnaire and the data classification section of the GRA to determine if there are any privacy issues that require attention, whether a data processing agreement (DPA) is needed (see below), and /or whether a data transfer mechanism is needed.

Legal Obligations

Data Processing Agreement

A data processing agreement (DPA) is a **written** contract between Adobe and its vendor for:

- **Processing:** Documents both parties' technical and administrative requirements for accessing, collecting, processing, transmitting, and storing personal information (we call this "processing")
- **Transferring:** Documents the data transfer requirements within its scope of services as described in the Master Agreement.
- **Securing:** Documents the technical and organizational controls to be implemented and maintained by vendor.

A DPA is required anytime there will be Processing of Personal Information. At Adobe, we require any vendor who will be receiving Restricted, Confidential, or Personal Information from us to sign a DPA. Vendors under a DPA agreement are required to adhere to the requirements as noted below.

- **Elements of the Adobe DPA:**
  - **Security** — Our DPA contains provisions that describe the minimum security requirements a vendor must comply with when handling Adobe Information. This includes issues such as when and how a vendor must notify Adobe of a Security Incident, minimum access controls a vendor must put around Adobe Information, security assessments it must undergo, logging requirements, etc.
  - **Privacy** — Our DPA also documents both Adobe's and the vendor's obligations under applicable data protection laws (including GDPR). More specifically, they address:
    - Processing — a vendor is only to Process or store Adobe Personal Information to the extent necessary to perform its obligations under the Master Agreement and in compliance with all applicable laws.
  - **Transfer** — A vendor who will access or store any Personal Information from outside the country of residence may be required to have a data transfer mechanism, depending on the country of origin:
    - If there will be access to EU Personal Information from outside of the EU/EEA, or transfer of EU Personal Information to a country outside of the EU/EEA, it must have a valid data transfer mechanism.
      - Adequacy (data accessed from or stored in an "adequate country)
      - Privacy Shield certification (only covers access to EU PI from or transfer of EU PI to the U.S.)
      - EU Model Clauses/Standard Contractual Clauses ("SCCs")
      - Processor Binding Corporate Rules ("BCRs")

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 Guardrails Risk Assessment program is a critical element in helping ensure that third-party vendors we do business with adheres to the same stringent information security standards as Adobe itself. By requiring vendors to comply with the Adobe Vendor Information Security Standard, Adobe employees and business owners can make informed decisions about entering into business relationships with third-parties that collect, store, process, transmit, or dispose of data for Adobe Internal, Confidential, or Restricted data outside of Adobe-controlled physical offices or data center locations. Adobe helps ensure ongoing compliance by requiring third-party vendors to sign a security addendum during the onboarding process. With the Guardrails program, Adobe helps ensure that its culture of security extends to the vendors with whom the company does business.

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com