Adobe Provider Data Processing Agreement:
Information Security and Privacy Terms

Effective as of August 29, 2022. These Terms replace and supersede all prior versions.

Adobe and Provider (the contracting entity as defined in the Agreement) have entered into an Agreement (the "Agreement") pursuant to the terms of which Provider may Process certain Adobe Information (as defined below) in connection with the Services. This document describes the specific data transfer and processing requirements (including without limitation, the security and privacy requirements) applicable to Provider's Processing of Adobe Information ("Security and Privacy Procedures"). Unless specifically defined in this document, capitalized terms shall have the meanings set forth in the Agreement.

1. **Definitions.**
   - **1.1** **"Adobe's Corporate Identity Provider"** means integrating with Okta as an Identity Provider (IdP) using the SAML 2.0 protocol for any user having an '@adobe.com' e-mail address (or successor technology approved by Adobe).
   - **1.2** "**Adobe Affiliate**" means an affiliate of Adobe (e.g., Magento, Marketo).
   - **1.3** **"Adobe Customer"** means a person who either independently or on behalf of a business entity is a customer of Adobe and/or an Adobe Affiliate.
   - **1.4** **"Adobe Information"** means any Adobe, Adobe Affiliate or Adobe Customer Confidential Information, Cardholder Information, Personal Information, or Sensitive Personal Information (including any information derived or inferred from such Adobe Information) that is Processed by Provider or Provider Parties in connection with the Services. In addition to Personal Information from Adobe Customers, Adobe Information may also include Personal Information from prospects, business partners, vendors, contractors, employees, agents, and advisors.
   - **1.5** **"Adobe Password Standards"** means the following minimum password requirements: (i) unique user identification; (ii) minimum 12-character password; (iii) includes at least one uppercase character, one lowercase character, one digit, and one special character; (iv) must be updated every 90 days; (v) access attempts limited to six within a five-minute period; and (vi) salted and hashed.
   - **1.6** **"Adobe Security Contact"** means the individual on the Adobe Information Security team that can be reached by email at scc@adobe.com in the event of a Security Incident.
   - **1.7** **"Cardholder Information"** means: (i) with respect to a payment card, the account holder's name, account number, service code, card validation code/value/number, PIN or PIN block, valid to and from dates and magnetic stripe data; and (ii) information relating to a payment card transaction.
   - **1.8** **"Confidential Information"** refers to that information defined as Confidential in the Agreement or in these Security and Privacy Procedures.
   - **1.9** **"Controller"** refers to the term as defined in applicable Data Protection Requirements, including without limitation, the GDPR and the Virginia Consumer Data Protection Act (2021).
   - **1.10** **"Data Protection Requirements**" means, collectively, any applicable international, national, state and local laws or regulations relating to the Processing and protection of Personal Information.
   - **1.11** **"European Personal Information"** means collectively (i) Personal Information that is subject to the data protection laws of the European Union, or of a member state of the European Union or EEA ("**EU Personal Information**"), (ii) the data protection laws of the United Kingdom ("**UK Personal Information**") and/or (iii) the data protection laws of Switzerland ("**Swiss Personal Information**"), and any successors or amendment thereto.

1.12 "**FADP**" means the Swiss Federal Act on Data Protection of 19 June 1992 and the Swiss Ordinance on the Federal Data Protection Act of 14 June 1993, and any new or revised version thereof that may become effective from time to time.

1.13 "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council.

1.14 **"Multifactor Authentication"** means authentication based on the use of at least 2 of the following forms of evidence: (i) something only the user knows (for example, a password or security question); (ii) something only the user possesses (for example, an authentication code sent to the user's device); and (iii) something inherent to the user (for example, keystroke recognition pattern).

1.15 **"Online Security Assessment"** means Adobe's Vendor Security Review, an online security risk assessment (or equivalent) for evaluation of Provider's security controls.

1.16 **"Personal Information"** means any information relating to an identified or identifiable natural person. An "identifiable natural person" means a person who can be identified, directly or indirectly, in particular, by reference to an identifier such as a name, an ID number, an online identifier etc. Personal Information includes 'personal data', 'special categories of personal data' and 'sensitive personal information or data' as defined under applicable Data Protection Requirements and may relate to any individual, such as a customer, employee, vendor, or contractor.

1.17 **"Processed" or "Processing"** means any operation or set of operations performed upon the Adobe Information or sets of Adobe Information, whether or not by automated means, such as access, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

1.18 **"Processor"** refers to the term as defined in applicable Data Protection Requirements, including without limitation the GDPR, UK GDPR and the Virginia Consumer Data Protection Act (2021). "Processor" shall also include "Service Provider" and "Contractor" as defined under the California Consumer Privacy Act (2018), as amended, where the processing activity relates to California consumers and Provider is processing Adobe Information on Adobe's behalf.

1.19 **"PCI Standards"** means the security standards for the protection of payment card data with which the payment card companies require merchants to comply, including the Payment Card Industry Security Standards currently in effect and as may be updated from time to time.

1.20 "**Protected Area**" means: (i) in the case of EU Personal Information, the member states of the European Union and the European Economic Area and any country, territory, sector or international organization in respect of which an adequacy decision under Art. 45 GDPR is in force; (ii) in the case of UK Personal Information, the United Kingdom and any country, territory, sector or international organization in respect of which an adequacy decision under United Kingdom adequacy regulations is in force; and (iii) in the case of Swiss Personal Information, any country, territory, sector or international organization which is recognized as adequate under the laws of Switzerland.

1.21 **"Provider Parties"** means any Provider employee, contractor, affiliate, or third-party entity that Provider uses to provide Services to Adobe under the Agreement.

1.22 **"Public Network"** means any data network established and operated that provides data transmission Services for public use, such as the Internet.

1.23 "**Relevant Applicable Law**" means a law to which a party is subject which may require or affect the Processing of Personal Information under the Agreement which, in the case of EU Personal Information shall mean any law of the European Union or a member state of the European Union or EEA, in the case of UK Personal Information shall mean any law of any part of the United Kingdom and in the case of Swiss Personal Information shall mean any law of Switzerland.

1.24 **"Secure FTP"** means "Secure File Transfer Protocol" which is a method used to encrypt and decrypt data that is transferred between a client and server, or a successor technology approved in writing by Adobe.

1.25 **"Security Incident"** means that Provider reasonably believes that: a) there is a substantial likelihood of accidental or unauthorized acquisition, destruction, loss, modification, use, or disclosure of, or access to, Adobe Information Processed by, or on behalf of, Provider; or malware was or is present on a Provider system in a manner that Adobe users were or may have been exposed to the malware (for example, malware was present on a Provider system from which end users download content whether or not such content was downloaded).

1.26 **"Services"** means services provided by Provider to or on behalf of Adobe as agreed to in the Agreement or corresponding order form.

1.27 **"Sensitive Personal Information"** means an individual's: (i) social security number, national identification number or equivalent, taxpayer identification number, passport number, driver's license number or other government –issued identification number; (ii) financial account number, with or without any code or password that would permit access to the account (such as bank account numbers and debit or credit card numbers); (iii) ethnicity or race information, religious, political or philosophical belief information, medical or health information, trade union membership information, details of criminal convictions or charges, biometric or genetic information (for purpose of uniquely identifying a natural person), background check information, sex life information (including sexual orientation); (iv) Cardholder Information; (v) any Personal Information defined as "Sensitive" (or equivalent) under an applicable Data Protection Requirement.

1.28 "**Standard Contractual Clauses**" or "**SCCs**" means:

a. in respect of EU Personal Information, the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914, including the text from module two (where Adobe is Controller of such Personal Information) or module three (where Adobe is Processor of such Personal Information on behalf of Adobe Customers and/or Adobe Affiliates) of such clauses and not including any clauses marked as optional ("**EU Standard Contractual Clauses**");

b. in respect of Swiss Personal Information, the EU Standard Contractual Clauses, provided that any references in the clauses to the GDPR shall refer to the FADP; the term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18(c) of the clauses; and the clauses shall also protect the data of legal persons until the entry into force of the revised FADP; and

c. in respect of UK Personal Information, the International Data Transfer Addendum to the EU Standard Contractual Clauses, issued by the Information Commissioner and laid before Parliament in accordance with s.119A of the Data Protection Act 2018 on 2 February 2022 but as permitted by Section 17 of such Addendum, with the format of the information set out in Part 1 of the Addendum amended as set out in Section 11.1.c ("**UK Addendum**").

1.29 "**Third Country**" means a jurisdiction outside of the Protected Area.

1.30 **"UK GDPR"** means the GDPR as amended by any legislation arising out of the withdrawal of the UK from the European Union and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (as amended).

2. Information Security Program: Technical and Organizational Measures.

2.1 In General. Provider must:

a. Develop, implement, maintain, and monitor a comprehensive, written information security program that contains appropriate administrative, technical, and physical safeguards to protect against anticipated threats or hazards to the security, confidentiality, availability, or integrity of Adobe Information, including the unauthorized or accidental acquisition, disclosure, destruction, loss, alteration, or use of, and the unauthorized access to, Adobe Information;

b. In assessing the appropriate level of security to be applied to the Adobe Information, take account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for data subjects and, in particular, ensure that additional safeguards and/or specific restrictions are applied to any Sensitive Personal Information being Processed by Provider;

c. Conduct routine risk assessments to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, availability, and integrity of electronic, paper, and other systems Processing Adobe Information and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting those internal and external risks;

d. Ensure that its information security program is consistent with: (i) these Security and Privacy Procedures; (ii) the Data Protection Requirements; and (iii) if Provider has access to or otherwise Processes Cardholder Information, the PCI Standards;

e. If Provider Processes Adobe Information in any way, ensure those with access to Adobe Information are authenticated via Multifactor Authentication. Multifactor authentication must also be used for access to environments that host production systems or systems and applications containing restricted and/or confidential data.

f. Provide reasonable assistance to Adobe in Adobe's assessment and implementation of appropriate technical and organizational measures to ensure an appropriate level of security of Adobe Information.

g. If Provider controls end user access to Adobe's network or systems, (i) implement industry-standard measures, including internet address protocol (IP) blocking technology, to prevent access to Adobe networks, systems, or information by users in embargoed countries (as identified in Country Group E:1 in Supplement No. 1 to Part 740 of the Export Administration Regulations (15 CFR Parts 730-774) or equivalent rules in the European Union, UK and other jurisdictions in which Adobe and Adobe Affiliates operate); and (ii) notify the Adobe Security Contact immediately by email when it has reasonable "knowledge": (as defined in the Definitions of Terms in Part 772 of the Export Administration Regulations (15 CFR Parts 730-774)) of any potential or actual activity involving access by users in Embargoed Countries to Adobe networks, systems, or information.

2.2 Provider Review of the Information Security Program. Provider shall review and update its information security program policies at least annually or whenever there is a material change in Provider's practices that may reasonably affect the security, confidentiality, availability, or integrity of Adobe Information. Provider may not alter or modify its information security program in such a way that will weaken or compromise the security of Adobe Information. If available, Provider will provide to Adobe (upon request) copies of its audited security assertions (SSAE18 SOC 2 Type 2 report, or, for Providers outside the United States, an ISO 27001 certificate, or international equivalent) on an annual basis.

2.3 Maintaining the Information Security Program. Provider shall maintain, train its workforce, and enforce its information security program at each location from which Provider provides the Services. Provider shall regularly conduct network vulnerability scans, penetration testing, and incident response tabletop exercises as part of its information security program. Provider's information security program shall cover all networks, systems, servers, computers, notebooks, laptops, PDAs, mobile phones, and any other devices or media that Process Adobe Information or that provide access to Adobe networks or systems.

Provider's information security program shall include industry standard password protections, firewalls, and anti-virus and malware protections to protect Adobe Information stored on computer systems. Provider shall have baseline security configurations or hardening images for firewalls, routers, servers, personal computers, wireless and remote access points and shall promptly install security relevant patches, including software or firmware updates in accordance with industry standard patch management protections.

2.4 Logging Requirement. Provider will automatically collect system, application, and user level logs on an ongoing basis. Logs must (at a minimum) contain username, location, date and time of access, IP address, and actions performed. Logs must be kept for a minimum of ninety (90) days and made available to Adobe for review within twenty-four (24) hours upon Adobe's request (in the event of a Security Incident) or within seventy-two (72) hours for all other requests unless otherwise agreed to in writing by Adobe. Provider must perform audit log collection and aggregation of all key web service systems and applications that are involved in the Processing of Adobe Information and monitor those logs for evidence of any Security Incident. Authentic copies of Adobe Information that has been accessed or acquired by an unauthorized person must be provided promptly to Adobe Security Contact upon request.

2.5 Adobe Security Assessments. Adobe may require Provider to complete periodic Online Security Assessments of Provider's computing systems, environments, and networks involved in the Processing of Adobe Information. Provider agrees that should the Online Security Assessment reveal a material issue in Provider's security or privacy controls, Adobe may suspend Provider's access to Adobe's computing systems and networks until such the relevant security or privacy control has been appropriately addressed. Such suspension will not be considered a material breach of the Agreement.

2.6 Magento Security, Privacy and Architecture. To the extent Provider will provide Services that could be integrated with or accessible from any version or type of Magento platform, server or instance (including any on-premise, cloud or open source instance of Magento), Provider will ensure that it maintains an equivalent or greater level of security and data protection for its systems, tools, interfaces, extensions, consoles and networks consistent with Adobe's Technical and Organizational Measures (https://www.adobe.com/go/CloudSvcsTOSM) as may be amended from time to time. Provider represents and warrants that it is not aware of any defect or vulnerability that could compromise the security of any Magento system, network or platform when integrated or connected with the Services.

2.7 Marketo Security, Privacy and Architecture. To the extent Provider will provide Services that could be integrated with or accessible from any version or type of Marketo platform, server or instance (including any on-premise, cloud or open source instance of Marketo), Provider will ensure that it maintains an equivalent or greater level of security and data protection for its systems, tools, interfaces, extensions, consoles and networks consistent with Marketo's Technical and Organizational Measures for Data Protection (https://www.adobe.com/go/CloudSvcsTOSM) as may be amended from time to time. Provider represents and warrants that it is not aware of any defect or vulnerability that could compromise the security of any Marketo system, network or platform when integrated or connected with the Services.

3. Processing, Disclosure, and Destruction of Adobe Information.

3.1 Role of the Parties. In accordance with all Data Protection Requirements, Provider is a Processor or sub-processor Processing Adobe Information on Adobe's behalf. Provider will ensure that the Processing of Adobe Information is carried out in compliance with Adobe's instructions as further set out below.

3.2 Processing of Adobe Information.

a. **Scope of Processing.** If applicable, the description of the Processing carried out by Provider is set out in the Agreement, the Online Security Assessment, and/or Annex I of the Schedule. Annex I of the Schedule, if applicable, shall be populated by the parties where such information is required to be set out in these Security and Privacy Procedures under Data Protection Requirements.

b. **Purpose of Processing.** The purpose of Processing under these Security and Privacy Procedures is the provision of the Services pursuant to the Agreement as may be further described by the applicable ordering documents or information submitted to Adobe as part of a vendor review. Annex 1 of the Schedule describes the subject matter and details of the Processing of Personal Information.

c. **Processing Limitation.** Provider may only Process Adobe Information (i) on Adobe's behalf; (ii) in accordance with Adobe's written instructions (which include the Agreement and these Security and Privacy Procedures and which may be given subsequently throughout the duration of the Processing under the Agreement); and (iii) for the sole purpose of providing, operating, managing, testing, maintaining and enhancing the Services and/or protecting the Services from a threat to the Services or to Personal Information. Provider is not permitted to sell Adobe Information or cause, allow, or facilitate the sale of Adobe Information. Except as necessary to provide the Services, Provider is not permitted to collect, retain, use, or disclose Adobe Information for its own purposes or for the purpose of any third party, firm, or enterprise (including affiliates). Provider is not permitted to combine Adobe Information with information from another customer or client, or that Provider collects from its own interactions with individuals, provided that Provider may combine personal information to perform any business purpose permitted or required under the Agreement to perform the Services as Processor or as otherwise permitted by Data Protection Requirements.

d. If Provider is required, under any Relevant Applicable Law, to process any Personal Information for any purpose other than that described in these Security and Privacy Procedures or the Agreement and more particularly at c. above, Provider will inform Adobe of this requirement first, unless such Relevant Applicable Law(s) prohibit this on important grounds of public interest.

e. **Record of Processing Activities.** Where required by applicable Data Protection Requirements, Provider and, where applicable, Provider Parties will maintain a written record of their Processing activities (including in electronic form) for Personal Information and Sensitive Personal Information carried out in connection with the Services. Such record will include:

    i Name and contact details of the Processor or Processors and of each Controller on behalf of which Provider is acting, and, where applicable, of any sub-processors (Provider Parties) and where applicable, of the Controller and Processor's representative, and the Processor's data protection officer;

    ii the categories of Processing carried out on Adobe's behalf;

    iii where applicable, transfers of Personal Information to a Third Country or an international organization, including the identification of that Third Country or international organization, and the documentation of appropriate safeguards; and

    iv where possible, a general description of the technical and organizational security measures.

f. **Assistance.** In accordance with the Data Protection Requirements, Provider shall take all reasonable and appropriate steps to assist Adobe in meeting Adobe's obligations under the Data Protection Requirements (including without limitation Articles 32 to 36 of GDPR/UK GDPR) taking into account the nature of the Processing under the Agreement, including with respect to any deidentified data, aggregated, or pseudonymized data.

g. **Infringing instructions**. Provider shall immediately inform Adobe if, in its opinion, Adobe's instructions infringe the Data Protection Requirements or makes a determination that it can no longer meet its obligations under these Security and Privacy Procedures or Data Protection Requirements in the timeframe required by such law.

3.3 Third Parties. To the extent Provider is a Third Party under the California Privacy Rights Act ("CPRA"), § 1798.100 et. seq., the following provisions shall apply instead of Section 3.2(c): The Provider receiving Adobe Information may process Adobe Information only for the limited and specified purposes set forth in the Agreement, including these Security and Privacy Procedures. The Provider must comply with all Data Protection Requirements, including all applicable sections of the CPRA and provide the same level of privacy protection as required of businesses by the CPRA. Among these, the Provider must comply with consumer requests to opt out of sale or sharing forwarded by Adobe. Where Provider is providing Services that include the collection of Personal Information on either Adobe's or Provider's behalf on an Adobe managed website, Provider shall check for and comply with the website visitor's opt-out preference signal unless otherwise informed by Adobe that such website visitor has consented to the sale or sharing of their Personal Information.

3.4 Disclosure of Adobe Information.

a. In General. Except as may be permitted pursuant to this Section 3.4, Provider may not disclose Adobe Information to any third party, firm, or enterprise (including an affiliate) in violation of the terms and conditions of the Agreement or this document.

b. Sub-processors. Provider may use Provider Parties in connection with the Services subject to the following requirements:

i. Provider must provide Adobe with a current list or link to its Provider Parties (excluding Provider employees) before disclosing Personal Information to any third party (including Provider Parties, but specifically excluding Provider's employees). The list must include the Provider Parties' country of location and instructions for communicating to Adobe any updates to this list.

ii. Provider shall inform Adobe in writing of any intended changes to such list at least 15 business days in advance (together with the information necessary to enable Adobe to exercise its right to object), thereby giving Adobe sufficient time to consider such change. Where Adobe has a reasonable basis to object to a new Provider Party, Adobe must promptly contact Provider in writing within 15 business days after receipt of such change. Adobe and Provider will work together without unreasonable delay to recommend an alternative arrangement. If a mutually acceptable and reasonable alternative arrangement is not found, Adobe may terminate the impacted Services without penalty.

iii. Provider must enter into a written agreement with the Provider Party prior to providing access to or otherwise disclosing Adobe Information. The written agreement must contain materially similar data protection obligations as those imposed upon Provider under these Security and Privacy Procedures.

iv. At Adobe's request, Provider shall provide a copy of such agreement (and any subsequent amendments) to Adobe (with terms redacted as may be necessary to protect business secrets or any other confidential information).

v. Provider shall notify Adobe of any material failure by any Provider Party to fulfil its obligations under such agreement.

vi. Provider shall ensure its Provider Parties materially comply with the obligations to which Provider is subject pursuant to these Security and Privacy Procedures, the Agreement and the Data Protection Requirements, and Provider is at all times accountable and responsible for the acts and omissions of its Provider Parties, with respect to the disclosed Adobe Information.

vii. Provider shall agree a third-party beneficiary clause in its agreement with the Provider Party whereby, in the event that Provider has factually disappeared, ceased to exist in law or has become insolvent, Adobe shall be entitled to terminate Provider's agreement with the Provider Party and to instruct the Provider Party to destroy or return the Adobe Information.

c. Response to Inquiries. Provider must: (i) unless prohibited by a Relevant Applicable Law, notify Adobe immediately (and in any event before any disclosures are made or access to Adobe Information is provided) if Provider receives an inquiry, complaint or request from any individual, entity, organization, law enforcement, regulatory or governmental official or court or other public authority related to or in connection with Adobe Information ("Request"); and (ii) seek to redirect the Request to Adobe (whilst providing reasonable support to Adobe to assist them in their response to such Request). Where (ii) is not possible, Provider shall (with Adobe's consent) assess the legality of the Request and use its best efforts to challenge the Request (this shall include informing any requesting public authority of any incompatibility of the Request with the safeguards contained in the Standard Contractual Clauses and the resulting conflict of obligations for Provider). Where such challenge is not possible, then Provider shall (with Adobe's consent) respond to any such Request within any specified timescale and will exercise best efforts to prevent and limit any such disclosure or access only to information that is expressly required in the Request and to preserve the confidentiality of the Adobe Information, including cooperating with Adobe to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to the Adobe Information. If the Request comes from law enforcement or other public authority, Provider shall (with Adobe's consent) notify any relevant data protection supervisory authority prior to such response. Where Provider is prohibited by any Relevant Applicable Law from notifying Adobe or any relevant data protection supervisory authority, Provider agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible to Adobe. Provider. Provider agrees to document its best efforts to challenge any Requests or waive any prohibitions, which should be available on request to Adobe. For the purposes of this Section 3.4.c, best efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of any relevant jurisdiction.

3.5 Return or Destruction of Adobe Information.

a. In General. If Adobe is not capable of removing or deleting Adobe Information from the Services, Provider will, at Adobe's request or upon the expiration or termination of the Agreement for any reason, promptly return to Adobe or destroy (and certify in writing to Adobe the destruction method used, the date of destruction and the party that performed the destruction), at Adobe's option, the Adobe Information that is in Provider's or Provider Parties' possession or control. If Adobe elects to have such information returned, Provider will return all such information via a bonded courier. Provider will destroy Adobe Information stored as a backup in accordance with its written policies and normal course of operations. If Provider does not have a written policy for destruction of backups, Provider will destroy Adobe Information stored in backup or archived form as mutually agreed between the parties. Provider will, upon Adobe's written request, certify in writing to Adobe the destruction method used, the date of destruction and the party that performed the destruction. Until the Adobe Information is destroyed or returned, Provider shall continue to ensure compliance with these Security and Privacy Procedures.

b. Disposal Methods. If Provider disposes of any paper, electronic, or other record containing Adobe Information, Provider will take all reasonable steps (based on the sensitivity of the Adobe Information) to destroy the Adobe Information by: (i) shredding; (ii) permanently erasing and deleting; (iii) degaussing; or (iv) otherwise modifying the Adobe Information in such records to make it unreadable and indecipherable. All Sensitive Personal Information must be disposed of in a manner described in (i) through (iii).

4. **Cardholder Information.** This section 4 is only applicable if Provider will Process Cardholder Information.
   - **4.1 In General.** If Provider has access to (or is permitted access to) Cardholder Information, Provider: (i) represents that its information security program addresses the requirements of the PCI Standards; (ii) maintains a complete audit trail of all transactions and activities associated with Cardholder Information; and (iii) does not store card validation codes/values/numbers, complete magnetic stripe data or PINs and PIN blocks.
   - **4.2 PCI Certification.** If Provider has access to Cardholder Information, Provider represents and warrants that it maintains certification of its compliance with the PCI Standards and that it regularly participates in independent, third-party monthly system vulnerability scans. Provider will promptly provide, at the request of Adobe, current certification of compliance with the PCI Standards, by an authority recognized by the Payment Card Industry for that purpose.

5. **Personnel Security**
   - **5.1 Confidentiality.** Provider will ensure Provider Parties with access to Adobe Information or who otherwise Process Adobe Information, are informed of the confidentiality requirements and have executed confidentiality agreements or have statutory or regulatory confidentiality obligations equivalent to the requirements of these Security and Privacy Procedures.
   - **5.2 Training.** Provider Parties with access to or who otherwise Process Adobe Information have received appropriate training regarding information security and data privacy.
   - **5.3 Criminal History.** Provider will not provide access to Adobe Information to any person who, to the best of Provider's knowledge, has been convicted of a crime (including, without limitation, any felony or misdemeanor) involving fraud or dishonesty in the past two years.

6. **Physical and Environmental Security.** Provider's information processing facilities that Process Adobe Information in any format (including Adobe Information maintained in paper or digital form) are housed in secure facilities and protected by perimeter security, such as barrier access controls that provide a physically secure environment from unauthorized access, damage, and interference, and surveillance and alarm systems.

7. **Access Control**.
   - **7.1 In General.** Provider has established and enforces written procedures that follow role-based access control principles to control the access to systems, networks, Services, and facilities that may Process Adobe Information. Provider will have a system in place to periodically review the users who have access to information systems that use or house Adobe Information to ensure that access privileges are relevant and appropriate for each individual user. No guest users or other anonymous/unidentified user accounts will be permitted. Provider will make such procedures available to Adobe upon request.
   - **7.2 "Need to Know" Access.** Provider will only grant access to the Adobe Information to members of its personnel to the extent strictly necessary for providing the Services and carrying out the Processing required thereunder.
   - **7.3 Access to Adobe Information.** Provider will limit access to Adobe Information to the minimum number of Provider Parties who require such access in order to provide the Services.
   - **7.4 Access to Adobe Network or Systems.** If Provider connects to Adobe's computing systems or networks, Provider agrees that: (i) Provider will not access, and will not permit any other person or entity to access, Adobe's computing systems or networks without Adobe's authorization and any such actual or attempted access will be consistent with any such authorization; and (ii) all Provider connectivity to

Adobe's computing systems and networks and all attempts at same will be only through Adobe's security gateways/firewalls and only for the purposes of providing the Services.

8. Communications and Operational Management.

8.1 In General. Provider shall monitor and manage each of its information Processing facilities, including, without limitation, implementing operational procedures, change management and incident response procedures, to ensure compliance with its obligations hereunder. For any significant changes to Provider infrastructure, data, software, and procedures that could affect the security of the Services provided to Adobe, Provider will communicate this to Adobe and get necessary approvals from Adobe before implementing these changes to production. Provider shall perform regular security and vulnerability scans no less frequently than monthly and shall remediate significant vulnerabilities as soon as possible, but within 30 days of discovery (or as mutually agreed in writing between the parties).

8.2 Anti-Malware Requirements. Provider shall implement anti-malware software on all systems that Process Adobe Information to ensure that all Adobe Information is free of malware (such as viruses, Trojan horses, worms, etc.), including laptops and other devices that Process Adobe Information. For Services that allow an end user to upload Adobe Information that is subsequently made available for download by an end user, Provider will scan the information for malware prior to making it available for download.

8.3 Encryption. Provider will encrypt all Adobe Information, using industry standard encryption tools such as AES-128 or equivalent encryption as defined by the most recent NIST standard, commonly implemented though protocols such as TLS, IPsec or Secure FTP, that Provider: (i) transmits or receives wirelessly or across Public Networks; (ii) stores on laptops; (iii) stores on storage media (e.g. servers, databases, backup tapes); (iv) stores on portable devices (such as USB drives, mobile and tablet devices); and (v) Processes on any device that is transported outside of the physical or logical controls of Provider including, any printer, copier, scanner, or fax machine. Provider will safeguard the security and confidentiality of all encryption keys.

8.4 Data Recovery. Provider has deployed and tested back-up facilities to ensure that Adobe Information may be recovered in the event of a disaster or media failure such as uninterruptible power supply and remote storage.

8.5 Email Notifications. If Provider originates email notifications to its users, Provider's domain must be compliant with Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) protocols before January 1, 2017, or at the start of Services. Provider is responsible for its email hygiene and Adobe shall not entertain whitelist requests. If Provider originates emails on behalf of Adobe (i.e., from an "…@adobe.com" email address), Provider must be compliant with the Domain-based Message Authentication, Reporting and Conformance (DMARC) protocol before June 1, 2017, or at the start of Services.

9. Security Incidents.

9.1 In General. Provider is responsible for managing Security Incidents involving Adobe Information that is Processed by, or on behalf of, Provider or Provider Parties. Provider will notify the Adobe Security Contact by email and by phone of any potential or actual Security Incidents without undue delay and in any event where (i) involving Personal Information within twenty-four (24) hours of the occurrence; or (ii) involving all other Adobe Information within seventy-two (72) hours of the occurrence. Provider will investigate the Security Incident and take all necessary steps to eliminate or contain the exposures that led to such Security Incident. Such notification shall contain at least the following information: a description of the nature of the Security Incident (including, where possible, the categories and

approximate number of data subjects and personal data records concerned); the details of a contact point where more information regarding the Security Incident may be obtained; and the likely consequences and the measures taken or proposed to be taken to address the Security Incident including to mitigate its possible adverse effects (and where it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay but in any event within the timeframes set out below).

Provider must provide Adobe with a written status update, via email, within seven (7) calendar days of the occurrence of any Security Incident, detailing mitigation steps taken by Provider in response to such occurrence and a final report detailing the investigation and remediation within ten (10) business days from the close of the Security Incident (or as mutually agreed in writing between the parties). Where any Security Incident involves or may involve Personal Information, Adobe may require such notification, status update and report to be provided by Provider within a shorter timeframe in order for Adobe to remain in compliance with any applicable Data Protection Requirements.

9.2 Provider Cooperation. Taking into account the nature of the Processing and the information available to Provider, it agrees to provide (at Provider's sole cost) reasonable assistance and cooperation requested by Adobe, in furtherance of any correction, remediation, or investigation of a Security Incident and/or mitigation of any damage, including any notification and/or credit reporting service that Adobe may determine appropriate to send to individuals impacted or potentially impacted by such Security Incident. Unless required by law, Provider will not notify any individual or any third party (including any national data protection authority or equivalent regulatory body) other than law enforcement of any potential Security Incident without first consulting with and obtaining the permission of Adobe.

10. Compliance; Right to Audit; Regulatory Requests; and Reasonable Assistance.

10.1 Compliance.

a. Each party shall ensure that it is able to demonstrate compliance with these Security and Privacy Procedures.

b. Provider shall deal promptly and fully with any inquiries from Adobe regarding the Processing of Adobe Information in accordance with these Security and Privacy Procedures.

c. Provider shall make available to Adobe all information necessary to demonstrate compliance with the obligations set out in these Security and Privacy Procedures which arise directly from the Data Protection Requirements.

10.2 Audits.

a. Provider will audit the security of the computers and computing environments that it uses in Processing Personal Information for the Services and the physical data centers from which Provider provides the Services. This audit (i) will be performed at least annually; (ii) will be performed by a third-party security professional (qualified auditor) at Provider's selection and expertise; (iii) will result in the generation of an audit report ("Audit Report") which will be Provider's Confidential Information; and (iv) may be performed for other purposes in addition to satisfying this requirement (as part of a regular internal security procedure).

b. Adobe is permitted to take reasonable and appropriate steps designed to ensure that Provider processes Adobe Information in a manner consistent with these Security and Privacy Procedures and Data Protection Requirements. Upon Adobe's written request (and no more than once per year), Provider will provide Adobe with a confidential summary of the most recent Audit Report with respect to Provider's commitments in these Security and Privacy Procedures ("Summary Report") so

that Adobe may reasonably verify Provider's compliance with these Security and Privacy Procedures. The Summary Report is Adobe Confidential Information.

c. Notwithstanding the above, at Adobe's request Provider shall permit and contribute to audits of the Processing activities, at reasonable intervals to be agreed between the parties (but no less than annually) or if there is, in Adobe's reasonable opinion, any indication of non-compliance by Provider. In deciding on whether to carry out an audit, Adobe may take into account any relevant certifications held by Provider. Adobe may conduct such audit itself or mandate an independent auditor. Any audit may include inspections at Provider's premises or physical facilities and shall, where appropriate, be carried out with reasonable notice.

d. Adobe and Provider shall make the information referred to in this Section 10.2, including the results of any audits and related reports, available to any national data protection authority or equivalent regulatory body on request.

10.3 Impact of Audit Requirements on Standard Contractual Clauses. In the event Standard Contractual Clauses are applicable, nothing in this Section 10 varies, modifies, or affects the Standard Contractual Clauses.

10.4 Reasonable Assistance: Correction, deletion, and blocking of data. To the extent Adobe does not have the ability to access Personal Information to respond to requests from individuals enforcing their right to correct, amend, port, or delete their data upon request (as permitted by Data Protection Requirements), Provider will assist Adobe with any reasonable request to do so within 7 business days of Adobe's request and at all times acting in compliance with Adobe's instructions. Adobe will supply Provider with information necessary for Provider to assist with such request upon Provider's written request. If an individual should communicate directly with Provider to request enforcement of their individual rights under Data Protection Requirements in connection with the Services provided to Adobe by Provider, Provider will promptly notify Adobe of the request and will provide Adobe with reasonable assistance in processing any such request (without responding to such request itself unless authorized in writing to do so by Adobe).

11. International Data Transfers and Processing of Personal Information.

11.1 Transfer of European Personal Information (if applicable).

a. If Provider Processes any European Personal Information outside of the Protected Area, Provider shall only do so with Adobe's prior written consent and in accordance with its written instructions and, where such prior written consent is granted, Provider will, for the duration of the Processing of European Personal Information, comply with the appropriate module of the Standard Contractual Clauses (either as a Processor where Adobe and/or Adobe Affiliates are Controllers (module 2) or as a sub-processor where Adobe and/or Adobe Affiliates have entered into SCCs with other Adobe Affiliates or Adobe Customers (module 3)) which Standard Contractual Clauses are hereby incorporated by reference into these Security and Privacy Procedures and the Agreement, with Adobe as the "data exporter" and Provider as the "data importer," and with the parties' signature and dating of the Agreement being deemed to be the signature and dating of the Standard Contractual Clauses and subject to the provisions of Sections 11.1.b and c. below;

b. For the purposes of the EU Standard Contractual Clauses (if applicable), the parties agree as follows:

i. for the purposes of clause 9(a) of the EU Standard Contractual Clauses, option 2 (General Written Authorization) applies with [15] business days as the notice period for any change to the list of sub-processors, as further set out in Section 3.4(b) of the Security and Privacy Procedures. Any notice pursuant to clause 9(a) of the EU Standard Contractual Clauses shall be submitted to DPO@adobe.com together with a description of the Processing by each such

sub-processor, categories of data subjects and the categories of Personal Information Processed, and the location of the Processing of Personal Information as well as any other information necessary to enable Adobe to decide whether to exercise its right to object;

ii. the information required by Annex I of the EU Standard Contractual Clauses is as set out in Annex I of the Schedule accompanying these Security and Privacy Procedures;

iii. the technical and organizational measures required by Annex II of the EU Standard Contractual Clauses (including information in relation to the technical and organizational measures in relation to data subject rights as required by clause 10(b) of the EU Standard Contractual Clauses) are as set out in these Security and Privacy Procedures and Annex II of the Schedule;

iv. any notice provided under clauses 9(d), 14(e) and 16 of the EU Standard Contractual Clauses shall be provided to DPO@adobe.com; and

v. for the purposes of clause 17 of the EU Standard Contractual Clauses, option 1 applies and the EU Standard Contractual Clauses shall be governed by the laws of Ireland and for the purposes of clause 18 of the EU Standard Contractual Clauses, the courts of Ireland shall have jurisdiction in relation to the EU Standard Contractual Clauses.

c. For the purposes of the UK Addendum (if applicable), the parties agree as follows:

i. the details of the parties in table 1 of the UK Addendum shall be as set out in the Schedule (with no requirement for signature);

ii. for the purposes of table 2, the UK Addendum shall be appended to the EU Standard Contractual Clauses (including the selection of modules and disapplication of optional clauses noted in Section 1.28 a above, and the option and timescales for clause 9(a) of the EU Standard Contractual Clauses noted in Section 11.1(b)(i) above);

iii. the appendix information in table 3 of the UK Addendum is set out in the Schedule; and

iv. for the purposes of table 4 of the UK Addendum, Adobe may end the UK Addendum as set out in Section 19 thereof.

d. The parties also agree to comply with the supplementary measures set out in Annex II of the Schedule, if applicable, to provide appropriate safeguards where EU or UK Personal Information is transferred to a Third Country.

e. The parties may agree to other mechanisms to transfer European Personal Information to Third Countries, where valid, under applicable Data Protection Requirements. Adobe may, at no cost, suspend or require Provider to suspend, any transfers of Personal Information which in Adobe's reasonable opinion do not comply or which cease to comply with Data Protection Requirements. In such case the parties shall negotiate in good faith a solution to enable the transfers of Personal Information to be reinstated in compliance with Data Protection Requirements. If Adobe and Provider (and any sub-processor, where relevant) are unable to promptly agree a solution, then Adobe shall have the right to terminate the Agreement in whole or in part by providing Provider written notice of termination which shall be effective as of the date of such notice of termination or such later date as determined by Adobe. The parties acknowledge and agree that a failure or a delay by Adobe to exercise its rights under this Section shall not constitute a waiver of these rights and does not prevent or restrict Adobe from exercising or further exercising its rights under this Section. No single or partial exercise of the rights under this Section shall prevent or restrict the further exercise of such rights.

11.2 All Other Transfers. If Provider accesses or Processes any Personal Information related to individuals residing outside of the Protected Area that are subject to cross-border data transfer requirements by applicable Data Protection Requirements, Provider will reasonably cooperate with Adobe to establish appropriate transfer mechanisms for such transfers.

11.3 Processing Personal Information. Provider agrees that it will only Process Adobe Information in compliance with applicable Data Protection Requirements. Provider shall take all appropriate legal, organizational, and technical measures to protect Personal Information in accordance with applicable Data Protection Requirements including those measures set out in these Security and Privacy Procedures and in particular having regard to the nature of the Personal Information.

11.4 Adobe Affiliates. Provider acknowledges that the provisions of this document are intended to inure to the benefit of Adobe Affiliates as third-party beneficiaries of this document, and the Adobe Affiliates will be entitled to enforce such provisions against Provider. Provider further acknowledges that the Adobe Affiliates accept their third-party beneficiary rights hereunder and that such rights will be deemed irrevocable. The respective rights and obligations of Provider under this document shall survive the termination, expiration, or other conclusion of the Agreement.

12. Miscellaneous

12.1 Provider Obligations. The obligations of Provider under this document shall continue for so long as Provider continues to Process Adobe Information, even if all agreements between Provider and Adobe have expired or been terminated.

12.2 Indemnification. Provider shall indemnify, hold harmless, and defend Adobe, its affiliates, and its and their officers, directors, employees, agents, successors, and assigns from and against any and all claims, losses, liabilities, damages, settlements, expenses and costs (including attorneys' fees and court costs) and any and all threatened claims, losses, liabilities, damages, settlements, expenses and costs arising from, in connection with, or based on allegations of, any of the following: (A) a material violation of the requirements of this document or the Data Protection Requirements; (B) a Security Incident; (C) the negligence or willful misconduct of Provider, Provider Parties or any third party to whom Provider provides access to Adobe Information or systems, with respect to security or confidentiality of Adobe Information; (D) remedial action taken by Adobe as the result of a Security Incident; and (E) any other costs incurred by Adobe necessary to enforce Adobe's rights in this document. Except as otherwise provided herein, Provider shall be fully responsible for, and shall pay, all costs and expenses incurred by Provider or Provider Parties with respect to the obligations imposed under this document.

12.3 Inability to Perform; Material Breach. In the event that Provider is unable to comply with the obligations stated in this document, is in substantial or persistent breach of any of its obligations under the Data Protection Requirements, or is unable to ensure Adobe Information is processed in accordance with Data Protection Requirements, or if Provider fails to comply with a binding decision of a competent court or a national data protection authority regarding its obligations under these Security and Privacy Procedures or Data Protection Requirements, Provider must promptly notify Adobe in accordance with Data Protection Requirements. If Provider is unable to ensure Adobe Information is processed in accordance with Data Protection Requirements, Provider grants Adobe the right to take reasonable and appropriate steps to stop and remediate unauthorized use of Adobe Information. Adobe may be entitled (at its option) to suspend the transfer of Adobe Information, require Provider to cease Processing relevant Adobe Information and/or immediately terminate the Agreement. Failure to materially comply with these Security and Privacy Procedures constitutes a material breach of the Agreement by Provider, entitling Adobe to the remedies provided for under the Agreement.

12.4 Termination by Adobe. Adobe may terminate the Agreement immediately as a result of a material failure by Provider to comply with the requirements of this document.

12.5 Trade Compliance. The parties agree that each may provide the other with access to information, products, technologies, or Services (hereafter referred to as "Item(s)") that may be subject to the trade control laws of the United States and other national governments regardless of where the Item is

received. Each party is responsible for complying with all applicable laws that may impact each party's right to import, export, or use the Items.

12.6 Precedence. In the event of any conflict or inconsistency between these Security and Privacy Procedures and the Standard Contractual Clauses referred to in Section 11, the Standard Contractual Clauses shall prevail.