PSLT - Adobe Primetime DRM (2017v1)

1. Additional Licenses and Restrictions.

1.1 **Licensed Product.** Adobe grants to Customer a non-exclusive, non-transferable, license to install and use the On-premise Software solely to develop and use the Licensed Product for the purpose of protecting and distributing Protected Content to a Customer Player, and creating Content Policies and Content Licenses for Customer's own account.

1.2 **Evaluation and Testing.** Customer may install and use the On-premise Software to develop and use the Licensed Product for the purposes of internal evaluation and testing the development of a Licensed Product. Any such evaluation deployment will use only evaluation Certificates issued by Adobe upon request by Customer. Distribution of Protected Content, Content Policies and Content Licenses using evaluation Certificates, to Consumers, other than employees of Customer, is prohibited without the prior written permission of Adobe.

2. License Restrictions and Customer's Obligations.

2.1 **Compliance and Robustness Rules; Verification Rights.** Customer must ensure that the Licensed Product complies with the Compliance and Robustness Rules at all times. If Adobe posts changes to the Compliance and Robustness Rules, Customer is required to comply with such changes as soon as commercially practicable, but no later than 6 months after the date the changes were posted. Customer is responsible for checking the web site listed in section 6.8 ("Compliance and Robustness Rules") of this PSLT periodically to be aware of any changes. Adobe will send notice of the change to the designated Certificate Administrator (as last provided by Customer), and notice will be considered received upon delivery to a properly addressed email. Lack of receipt of such notification will not exempt Customer from the obligation to comply with the then-current rules within the required period. In addition to the License Compliance section of the General Terms, Adobe may also inspect Customer's books, records, procedures and facilities as necessary to verify Customer's compliance with the Compliance and Robustness Rules.

2.2 **Content Protection Updates.** If Adobe delivers a Content Protection Update to Customer, Customer will apply such update to the On-premise Software, and discontinue using copies of the On-premise Software that have not been updated, as soon as reasonably possible and will provide notice to Adobe if this will take more than 90 calendar days.

2.3 **Certificate Expiration and Renewal**. Each Certificate for commercial use shall expire 2 years from the date it is generated by Adobe. Each Certificate for evaluation use shall expire 1 year from the date it is generated by Adobe. Customer will be required to place an order for new Certificates, as needed.

2.4 **No Circumvention**. No element of the On-premise Software may be used to circumvent or defeat the Content Protection Functions or other security requirements of the On-premise Software, and related technical specifications, provided hereunder. Customer must not (A) use Confidential Information or Highly Confidential Information to circumvent the Content Protection Functions of either the On-premise Software or any related Adobe Technology that is used to encrypt or decrypt digital content for authorized consumption, or (B) develop or distribute products that are designed to circumvent the Content Protection Functions of the On-premise Software or the content protection functions of any related Adobe Technology that is used to encrypt or decrypt digital content for authorized consumption.

2.5 **Viral Open Source**. Except as expressly permitted under this Agreement, Customer must not integrate, combine, or otherwise use, any software that is licensed under a VOSL with the On-premise Software, or take any other action that could require Adobe to disclose, distribute, or license all or any part of the On-premise Software in source code form, for the purpose of making derivative works, or redistributing at no charge. For the purposes of this section, "VOSL" or "Viral Open Source Licenses" means the GNU General Public License (GPL), GNU Affero General Public License (AGPL), GNU Lesser General Public License (LGPL), or any other license that requires (as a condition of use, modification or distribution) that software be: (A) disclosed or distributed in source code form; (B) licensed for the purpose of making derivative works; or (C) redistributed at no charge.

2.6 **Confidential Treatment of Content Encryption Keys.** Content Encryption Keys are Confidential Information. However, Customer will have no further confidentiality obligation for Content Encryption Keys that have been distributed to Consumers in Content Licenses.

3. Additional Terms for the Handling of Highly Confidential Information. Private Keys are subject to requirements applicable to Highly Confidential Information contained in the Compliance and Robustness Rules and any updates thereto, together with the following provisions (the "**Security Requirements**")**.**

3.1 All Authorized Employees must sign, or have signed, confidentiality agreements with Customer containing terms at least as restrictive as those in this section 3 and the Security Requirements, either as a condition of their employment or before they are granted access to the Highly Confidential Information. Customer shall ensure that all Authorized Employees are made aware of their obligation to comply with the Security Requirements. Customer shall promptly provide Adobe with copies of such confidentiality agreements signed by the Authorized Employees, if requested as part of any security verification permitted under section 2.1, above. Customer is fully responsible for the conduct of its employees (including Authorized Employees) who may in any way breach this section 3. Customer will, upon request of Adobe, take all reasonable steps necessary to recover any Highly Confidential Information and will bear the cost of such steps. Customer agrees to notify Adobe in the event of any breach of the terms of this section 3.1, including breaches in its security. Customer must cause each Authorized Employee to strictly abide by their obligations under this section 3 and the Security Requirements. Customer must use the same efforts to enforce the confidentiality obligations of each Authorized Employee after the termination of his/her employment as Customer uses to enforce its own confidential information, such efforts of enforcement not to be less than reasonable efforts.

3.2 Without limitation to any requirement of this section 3 and the Security Requirements, Customer agrees that it will treat the Highly Confidential Information with at least the same degree of care as it gives to the protection of its most sensitive confidential information, if any, and Customer represents that it exercises at least a high degree of care to protect its own such confidential information.

3.3 Customer's obligations with respect to the Highly Confidential Information are in effect in perpetuity. Customer's obligations not to disclose Highly Confidential Information shall not be subject to any of the exceptions set forth in the sections titled "Definition of Confidential Information" and "Confidentiality" of the General Terms, with the exception of the sub-section titled "Permitted Disclosure" under the section titled "Confidentiality" regarding disclosure required by law or the order of a court or similar judicial or administrative body.

4. Certificates Administration. Customer must provide Adobe with the name of one employee to serve as the "**Certificate Administrator**" responsible for administering the names of those Authorized Employees of Customer who are permitted to request Certificates from Adobe on behalf of the Customer. No Certificates will be delivered until a Certificate Administrator has been designated and Authorized Employees have been identified. The Certificate Administrator is prohibited from requesting Certificates. Customer may update the

name of the Contract Administrator from time to time during the Term, but no more than 3 times in a 12-month period, unless expressly approved by Adobe.

5. Remedies and Revocation.

5.1 **Revocation of Certificates**. Adobe will have the right to take measures to revoke Certificates ssued to Customer if Adobe obtains or becomes aware of evidence satisfactory, in Adobe's sole discretion, to establish that one or more of the following criteria are met:

(A) such Certificate or the Public Key associated with it is being used without authorization by a party other than the Customer to which it was issued by Adobe;

(B) the Private Key corresponding to a Public Key for which Adobe has issued a Certificate has been made public, lost, stolen, intercepted or otherwise misdirected, disclosed;

(C) revocation has been ordered by a court or similar judicial or administrative body of any government;

(D) the PSLT has expired or been terminated by either party; or

(E) Customer has requested or consented in writing to such expiration.

5.2 **Revocation Process**. If Adobe determines that any of the prior criteria have been met, Adobe will take reasonable steps to consult with Customer prior to initiating such revocation to determine if Customer can present evidence satisfactory to Adobe, in Adobe's sole discretion, that the relevant criteria have not been met and/or that revocation is not necessary to prevent any material compromise to the security of Protected Content or of the Content Protection Functions of the On-premise Software, or the content protection capabilities of any other Adobe On-premise Software as applied to any digital content. Adobe will not initiate such revocation prior to 30 days following notice of such consultation unless Adobe determines, in its sole discretion, that immediate or earlier revocation is necessary to mitigate ongoing and material harm to the interests of distributors of digital content protected using Adobe On-premise Software.

5.3 **Injunctive Relief**. In addition to the "Injunctive Relief" section of the General Terms, Customer agrees that certain breaches of this PSLT, including but not limited to breaches of sections 3, 4 and 5, of this PSLT and breaches of the Compliance and Robustness Rules, may compromise the Content Protection Functions of the On-premise Software and cause unique and lasting harm to the interests of Adobe and owners of Content that rely on such Content Protection Functions, and that monetary damages will be inadequate to compensate fully for such harm. Customer further agrees that Adobe will be entitled to obtain timely injunctive relief to prevent or limit the harm caused by such breaches, in addition to monetary damages or other remedies available at law.

6. Definitions.

6.1 **"Ad(s)**" means a graphic or multi-media file served in adjacent to or otherwise in connection with Customer Content, including, without limitation, overlays, companion banners, pre-roll/mid-roll/post-roll, video and display.

6.2 **"Authorized Employees"** means only those employees authorized to place or approve orders for Certificates through the online registration process for Certificate ordering as described in the Documentation, all of whom must at all times be full-time employees of Customer with a strict need to have access to Highly Confidential Information in order to perform Customer's obligations or exercise Customer's rights under this PSLT.

6.3 "**Authorized Site(s)**" means those Developments Site(s) identified in a Sales Order that may use and store Highly Confidential Information, subject to the terms of this PSLT and the General Terms.

6.4 "**Adobe Primetime DRM** means:

(A) the SDK and Documentation provided to Customer by Adobe under this PSLT that combines object code, and Certificates for the sole purposes of creating Protected Content, Content Licenses and Content Policies;

(B) any updates and fix releases thereto that Adobe may provide to Customer under this PSLT; and

(C) any other documentation or source or object code provided by Adobe under this PSLT that is intended to assist Customer in development of the Licensed Product.

6.5 "**Adobe Primetime TVSDK**" means Adobe's proprietary SDK for creating desktop and mobile application players of Content and Ads.

6.6 "**Certificates**" means electronic documents provided by Adobe under this PSLT that incorporate a digital signature that associates a public key with an entity (including server, client) and can be used to establish a chain of trust.

6.7 "**Certificate Revocation List (or CRL)**" means electronic documents published by Adobe to identify Certificates that are no longer valid, having been revoked by Adobe.

6.8 **"Compliance and Robustness Rules**" means the document setting forth compliance and robustness rules for the Licensed Product and use of the On-premise Software and Certificates located at http://www.adobe.com/go/FlashAccessComplianceandRobustnessRules or a successor web site thereto.

6.9 "**Consumer**" means an individual end user that receives Protected Content and obtains a Content License in order to obtain access to and view the Protected Content on a supported Customer Player.

6.10 "**Content**" for the purposes of this PSLT, means any and all audio, video, multimedia, text, images, documents, computer programs, data and any other information or materials. The definition of Content does not include Ads.

6.11 "**Content Encryption Key**" means a cryptographic value for use in encrypting Customer Content for secure distribution and for use by Customer Player to decrypt Protected Content for access and use in accordance with a Content License.

6.12 "**Content License(s)**" means metadata (stored on a computer and/or embedded in an electronic file delivered to a Customer Player) that:

(A) contains an encrypted Content Encryption Key; and

(B) contains or refers to usage rules for Protected Content designed to be enforced directly through the Adobe Primetime DRM technology incorporated into Customer Player.

6.13 "**Content Policy**" means metadata that contains usage rules for Protected Content.

6.14 **"Content Protection Functions**" means those aspects of the On-premise Software that are designed to implement requirements of the Compliance and Robustness Rules and/or prevent unauthorized access to Private Keys, Content Encryption Keys and Certificates or unauthorized access to or use of Protected Content inconsistent with the access and usage rules contained in a Content License or Content Policy associated with such Protected Content.

6.15 **“Content Protection Update**" shall mean an update to the On-premise Software that is designated as such by Adobe because it alters the prior means for providing the Content Protection Functions in the On-premise Software.

6.16 “**Customer Player**” means the video players that Customer created using the Adobe Primetime TVSDK under a valid license from Adobe.

6.17 “**Deliver or Delivery**” means to deliver or otherwise make available, directly or indirectly, by any means, Protected Content to one or more Consumers.

6.18 “**DRM Metadata**” means a data structure that contains the URL of a License Server and may contain the encrypted Content Encryption Key and/or a Content Policy.

6.19 “**Highly Confidential Information**” means Private Keys generated and controlled by the Customer for the purpose of creating Protected Content or issuing Content Licenses.

6.20 “**License Server**” means that portion of a Licensed Product that generates and issues Content Licenses.

6.21 “**Licensed Product**” means the software solution for creating Protected Content, Content Licenses and Content Policies developed by Customer using the On-premise Software.

6.22 “**Packager**” means a software utility that can create Protected Content and DRM Metadata that is derived from, or provided with, the On-premise Software, or that is separately licensed from Adobe, including the Adobe Primetime Streaming Server.

6.23 “**Private Key**” means a cryptographic value generated by the Customer and uniquely associated with a Public Key.

6.24 “**Protected Content**” means Content encrypted by a Content Encryption Key using a Packager.

6.25 “**Public Key**” means a cryptographic value generated by the Customer and uniquely associated with a Private Key that is incorporated into a Certificate issued by Adobe when Customer follows the Certificate generation process described in the Documentation.