CPP – Services On-demand pour Marketo Engage (2020v1)

1. **Respect des Règles applicables.**

   1.1 Le Client s'assurera que tous les Utilisateurs respectent les Règles applicables. « Règles applicables » désigne toutes les lois, directives, réglementations, codes et règles ainsi que la Politique d'utilisation acceptable pour Adobe (disponible sur https://www.adobe.com/legal/terms/aup.html ou tout site Web qui lui succéderait) applicables à l'utilisation des Produits et Services par le Client.

   1.2 Le Client reconnaît qu'Adobe n'agit qu'en qualité de « processeur de données » au nom du Client et que le Client est le « contrôleur des données » ou assume un rôle équivalent en vertu des lois applicables en matière de protection de la vie privée ou de protection des données (y compris le Réglement Général sur la Protection des Données si le Client est un résident de l'Union européenne).

   1.3 Le Client obtiendra toutes les habilitations, autorisations et approbations nécessaires de la part de toutes les personnes que le Client ou ses Utilisateurs contactent par le biais ou à la suite de l'utilisation des Services On-demand conformément aux Règles applicables à l'égard des données collectées, intégrées ou téléchargées par le biais des Services On-demand.

2. **Documentation.** Aux fins des présentes CPP, le terme « Documentation », tel qu'il est défini dans les Conditions Générales, comprend également la spécification technique applicable et la documentation d'utilisation des Produits et Services généralement disponibles sur https://docs.marketo.com.

3. **Droits d'Utilisation.** Le Client n'utilisera pas les Services On-demand au-delà des conditions d'utilisation spécifiées dans le Bon de Commande (ces conditions d'utilisation sont dénommées les « Droits d'Utilisation »). Si Adobe considère que le Client dépasse ses Droits d'Utilisation, Adobe en informera le Client par écrit ou par e-mail en identifiant le dépassement de ces Droits d'Utilisation, et le Client réduira sans délai son utilisation des Services On-demand dans les limites de ces Droits d'Utilisation. Si le Client ne s'y conforme pas dans les 30 jours, Adobe aura le droit de facturer au Client, et le Client acceptera de payer, les frais applicables à un niveau d'utilisation supérieur, dont les échéances seront harmonisées avec la Durée de la Licence dans le Bon de Commande applicable.

4. **Conservation et destruction des données.** Le Client peut supprimer ou conserver des Données du Client pendant la Durée de la Licence, sous réserve des Droits d'Utilisation applicables. Après la résiliation du Contrat, Adobe supprimera et détruira irrémédiablement les Données du Client et, sur demande écrite, Adobe certifiera ladite destruction.

5. **Erreurs de remise.** Adobe décline toute responsabilité en l'absence de remise des courriers électroniques imputable à des erreurs dans les adresses électroniques, aux avis de non-distribution définitive ou temporaire, aux filtres appliqués aux courriers électroniques par les clients, aux listes noires d'adresses électroniques et/ou à toute autre cause similaire. L'ensemble ou toute partie de ce qui précède peut également avoir une incidence négative sur les performances de livraison des courriers électroniques du Client dans le cadre de l'utilisation des Services On-demand par le Client et, dans ce cas, Adobe ne saurait être tenu responsable envers le Client ou un tiers d'une telle incidence négative.

6. **Résiliation des Services Professionnels.** Adobe peut résilier les Services Professionnels moyennant un préavis écrit de trente (30) jours adressé au Client si les performances du Client en vertu d'un Bon de Commande applicable retardent ou empêchent Adobe d'exécuter ses obligations en temps voulu ou de manière efficace.

7. **Restrictions de la licence.** Outre les conditions des licences accordées au Client et les restrictions de licence énoncées dans les Conditions Générales, le Client s'abstiendra et veillera à ce que les Utilisateurs n'utilisent pas ou n'accèdent pas aux Produits et Services pour construire, soutenir et/ou aider un tiers à construire ou soutenir des produits ou services concurrents des Services On-demand. Si le Client concède sous licence un déploiement des Services On-demand conforme au HIPAA : (a) le Client ne doit pas intégrer les Services On-demand à des Produits et Services non conformes au HIPAA ; et (b) le Client doit acheter le cryptage des données au repos pendant toute la Durée de la Licence de tous les Bons de Commande.

8. **Modifications du Produit.** Adobe se réserve le droit de modifier ou d'interrompre les fonctionnalités individuelles des Services On-demand. Le Client sera informé de ces changements ou interruptions via le portail des Services On-demand.

9. **Traitement et catégories de données à caractère personnel. Sécurité du traitement.**

9.1 Mesures de sécurité et Traitement des données. Les Réclamations liées à la sécurité et les Réclamations liées à la confidentialité des données des Conditions Générales ne s'appliqueront au Client uniquement dans la mesure où ce dernier achète, moyennant des frais supplémentaires, un dispositif de cryptage de haut niveau pour les données au repos pendant toute la Durée de la Licence de tous les Bons de Commande du Client.

9.2 Le Contrat de Traitement des Données (le cas échéant et ci-après le « DPA ») est modifié par la présente en ajoutant ce qui suit à la fin de l'Article 3 (Traitement et types de données personnelles) : « Uniquement en ce qui concerne les Services On-demand pour Marketo Engage : (a) Adobe traite toutes les Données du Client qui peuvent contenir des Données Personnelles dans les endroits décrits dans la « Liste des sous-traitants de Marketo » disponible sur : https://documents.marketo.com/legal/sub-processor-list ; et (b) l'objet, la nature et la finalité du traitement des données, le type de Données Personnelles ainsi que les catégories de personnes concernées sont conformes au Contrat, et comme le décrit plus spécifiquement la Documentation applicable. » Toute référence à la liste des sous-traitants dans ledit DPA fera plutôt référence aux sous-traitants figurant sur la Liste des sous-traitants ultérieurs de Marketo (tels que définis dans l'extrait ci-dessus).

9.3 Toute référence dans le DPA (le cas échéant) à « Adobe Inc. », « Adobe US » ou « Adobe » dans le cadre du Bouclier de protection des données UE-États-Unis, du Bouclier de protection des données Suisse-États-Unis et/ou des Clauses Contractuelles Types fera plutôt référence à « Marketo, Inc ».

9.4 Adobe a mis en œuvre et maintient des mesures techniques et organisationnelles afin de garantir un niveau de sécurité du traitement des Données du Client relatives aux Produits et Services Marketo Engage d'Adobe adapté au risque, comme indiqué dans les Mesures Techniques et Organisationnelles de Marketo Engage ci-jointes (les « Mesures Techniques et de Sécurité de Marketo Engage »). Toute référence dans le DPA (le cas échéant) aux Mesures Techniques et Organisationnelles d'Adobe se rapportera aux Mesures Techniques et de Sécurité de Marketo Engage.

Mesures Techniques et Organisationnelles de Marketo Engage

1. Contrôles et dispositifs de sécurité

1.1. Adobe se conformera à toutes les lois et réglementations applicables en matière de confidentialité et de sécurité des données régissant son utilisation, son traitement et son stockage des Données du Client.

1.2. Pendant la Durée de la Licence, Adobe doit maintenir un programme de sécurité aligné matériellement sur les normes industrielles applicables conçues pour assurer la sécurité, la confidentialité, la disponibilité et l'intégrité des Données du Client et se protéger contre la divulgation ou l'accès non autorisés aux Données du Client. Un tel programme de sécurité doit comprendre la mise en œuvre de mesures de protection administratives, techniques et physiques appropriées pour le type d'informations qu'Adobe traite et le besoin de sécurité et de confidentialité de telles informations.

1.3. Adobe met en œuvre des contrôles alignés sur les normes du secteur destinés à assurer la sécurité des Données du Client et, pendant toute la Durée de la Licence, doit maintenir des mesures de sécurité conçues pour : (i) protéger la sécurité des systèmes d'Adobe qui interagissent avec les Données du Client ; (ii) se protéger contre toute menace ou tout danger anticipé pour la sécurité ou l'intégrité des systèmes d'Adobe qui interagissent avec les Données du Client et (iii) se protéger contre l'accès ou l'utilisation non autorisés des systèmes d'Adobe qui interagissent avec les Données du Client et qui pourraient nuire aux Utilisateurs des Services On-demand du Client.

1.4. Adobe maintient des contrôles d'accès qui comprennent, sans s'y limiter, les éléments suivants :

1.4.1. Limiter l'accès à ses systèmes d'information et aux installations dans lesquelles ils sont logés à des personnes dûment autorisées ;
1.4.2. L'accès du personnel d'Adobe aux Données du Client est supprimé en cas de cessation d'emploi ou de changement de statut professionnel, auquel cas le personnel n'aurait plus besoin d'accéder aux Données du Client ;
1.4.3. Les mots de passe du système sont conformes à des normes de mots de passe strictes (9 caractères minimum) qui incluent la longueur, la complexité et l'expiration. Jusqu'à dix (10) tentatives de mot de passe peuvent être réalisées, après quoi l'accès est bloqué jusqu'à ce que le mot de passe soit réinitialisé par le personnel autorisé. Les politiques en matière de mots de passe sont conformes à la publication spéciale 800-53 du NIST ; et
1.4.4. L'accès est limité à ses systèmes d'information en utilisant une authentification multifactorielle.

1.5. Toutes les communications clients transmises sur Internet sont cryptées. Adobe utilise le cryptage sur ses propres serveurs de messagerie pour assurer un cryptage point à point via TLS opportuniste. Le Client peut choisir, moyennant un supplément de prix, de configurer les Services On-demand pour utiliser des canaux cryptés pour sa propre collecte de données via les pages d'accueil et à partir de l'activité de l'utilisateur sur le site Web du Client. Le Client peut choisir d'appliquer un cryptage de haut niveau aux données au repos moyennant des frais supplémentaires. Toutes les sauvegardes sont cryptées avec un cryptage de haut niveau.

1.6. Adobe surveille son réseau et ses systèmes de production, met en œuvre et maintient des contrôles et des procédures de sécurité conçus pour prévenir, détecter et répondre aux menaces et risques identifiés. Ces contrôles et tests comprennent notamment les éléments suivants :

1.6.1. Employer un système de détection d'intrusion réseau conforme aux normes de l'industrie pour surveiller et bloquer le trafic réseau suspect ;
1.6.2. Examiner les journaux d'accès sur les serveurs et les événements de sécurité et conserver les journaux de sécurité du réseau pendant 180 jours ;
1.6.3. Examiner tous les accès aux systèmes de production ;
1.6.4. Réaliser régulièrement des évaluations de vulnérabilité du réseau. Les analyses seront réalisées à

l'aide d'outils d'analyse conformes aux normes de l'industrie qui identifient les vulnérabilités des applications et des environnements d'hébergement. Adobe doit maintenir un programme de correction des vulnérabilités ; et

1.6.5. Engager des tiers pour réaliser des tests de pénétration du réseau au moins une fois par an.

1.7. Adobe doit s'assurer que :

1.7.1. Tous les terminaux utilisent une solution antivirus et appliquent des mises à jour de signature en temps opportun ; et

1.7.2. Toutes les vulnérabilités critiques exploitables sont corrigées en temps opportun.

2. Utilisations et divulgations des Données du Client. Adobe n'utilisera ni ne divulguera les Données du Client, sauf si cela s'avère nécessaire pour fournir les Services On-demand ou s'il en est stipulé autrement dans le Contrat.

3. Notification de violation de la sécurité. Adobe doit informer le Client dans les soixante-douze (72) heures suivant la prise de connaissance d'une acquisition, destruction, perte, modification, utilisation ou divulgation non autorisée et confirmée des Données du Client (« Violation de la sécurité »).

3.1. Adobe enquêtera et prendra les mesures raisonnablement nécessaires pour éliminer ou contenir les expositions qui ont conduit à une telle Violation de la sécurité.

3.2. Adobe fournira dès que possible au Client une description écrite de la Violation de sécurité et des mesures d'atténuation prises par Adobe.

4. Rapports d'audit. Adobe obtiendra des rapports d'attestation relatifs à son programme de sécurité de l'information (SSAE 16, SOC 2 ou un rapport équivalent) au moins une fois par an et conservera ces rapports pendant au moins trois (3) ans après chaque attestation.

5. Sensibilisation et formation à la sécurité. Adobe exige au moins une formation annuelle sur la sécurité et la confidentialité pour l'ensemble de son personnel.

6. Continuité des activités et reprise après sinistre

6.1. Adobe a mis en place des politiques et des procédures pour répondre à une urgence ou à tout autre événement (par exemple, incendie, vandalisme, défaillance du système, pandémie et catastrophe naturelle) qui pourrait affecter la disponibilité, l'intégrité ou la confidentialité des Données du Client ou des systèmes de production qui contiennent des Données du Client ou qui interromprait la capacité d'Adobe à fournir des Services On-demand en vertu du Contrat.

6.2. La protection des données, la haute disponibilité et la redondance intégrée d'Adobe sont conçues pour assurer la disponibilité des applications et protéger les informations contre toute perte ou destruction accidentelle. Le plan de récupération après sinistre d'Adobe comprend un basculement géographique entre ses centres de données américains. La restauration des Services On-demand s'inscrit dans le cadre d'efforts commercialement raisonnables et est effectuée conjointement avec la capacité d'un fournisseur de centre de données à fournir une infrastructure adéquate sur le lieu de basculement prédominant.

6.3. Adobe s'appuie sur les multiples niveaux de redondance de l'alimentation, de l'alimentation sans interruption (UPS) et de l'alimentation de secours des fournisseurs de centres de données ayant une bonne réputation pour le système d'Adobe contenant les Données du Client. Les systèmes d'alimentation des centres de données traitant les Données du Client sont conçus pour fonctionner sans interruption lors d'une panne totale d'électricité, chaque serveur recevant une alimentation UPS conditionnée. Le sous-système d'alimentation de l'UPS est redondant, avec basculement instantané en cas de panne de l'UPS primaire. Tous les fournisseurs de centres de données d'Adobe sont certifiés ISO 27001:2013.

6.4. Les installations de centres de données contenant les Données du Client disposent de systèmes avancés d'extinction d'incendie et de systèmes redondants de chauffage, de ventilation et de climatisation, permettant ainsi un flux d'air, une température et un taux d'humidité appropriés et constants.

6.5. Sauvegarde et récupération. Les installations des centres de données aux États-Unis utilisent des dispositifs d'instantané et de mise en miroir des données. L'intégrité des sauvegardes locales est testée trimestriellement en restaurant une base de données complète à partir d'une copie d'instantané sélectionnée pour tester les systèmes et valider l'intégrité des données. Les données du centre de données britannique sont sauvegardées quotidiennement sur des bandes et les données du centre de données australien sont sauvegardées électroniquement quotidiennement. Les processus de sauvegarde des installations des centres de données britanniques et australiens sont testés trimestriellement. Les données de sauvegarde ne sont pas transférées au niveau international.

6.6. Redondance du réseau et du stockage. L'infrastructure SaaS est conçue et construite pour une haute disponibilité. Tous les appareils réseau, y compris les pare-feux, les répartiteurs de charge et les commutateurs sont entièrement redondants et hautement disponibles. La haute disponibilité de la connectivité Internet est assurée par de multiples connexions dans chaque centre de données à différents FAI.