Conditions de traitement des données Google Ads

Google et la partie co-contractante acceptant les présentes conditions (« **Client** ») ont conclu un accord pour la fourniture des Services de sous-traitance (ci après « **l'Accord** », tel que modifié périodiquement).

Les présentes Conditions de traitement des données Google Ads (y compris les annexes, « **Conditions de traitement des données** ») sont conclues par Google et le Client et complètent l'Accord. Les présentes Conditions de traitement des données entreront en vigueur et remplaceront toutes les conditions précédemment applicables relatives à leur objet (y compris tout avenant ou addendum de traitement des données relatif aux Services de sous-traitance), à compter de la Date d'entrée en vigueur des Conditions.

Si vous acceptez les présentes Conditions de traitement des données au nom du Client, vous garantissez que : (a) vous avez la pleine capacité juridique pour engager le client au respect des présentes Conditions de traitement des données ; (b) vous avez lu et compris les présentes Conditions de traitement des données ; et (c) vous acceptez, au nom du Client, les présentes Conditions de traitement des données. Si vous n'avez pas la capacité juridique d'engager le Client, veuillez ne pas accepter les présentes Conditions de traitement des données.

1. Introduction

Les présentes Conditions de traitement des données reflètent l'accord des parties sur les conditions régissant le traitement et la sécurité des Données personnelles du Client dans le cadre de la Législation en matière de protection des données.

2. Définitions et Interprétation

2.1 Dans le cadre des présentes Conditions de traitement des données :

« **Produit supplémentaire** » désigne un produit, un service ou une application fourni par Google ou un tiers qui : (a) ne fait pas partie des Services de sous-traitance ; et (b) est accessible pour une utilisation dans l'interface utilisateur des Services de sous-traitance ou est autrement intégré avec les Services de sous-traitance.

« **Société affiliée** » désigne une entité qui, directement ou indirectement, contrôle une partie, est contrôlée par elle ou est sous contrôle commun avec elle.

« **Données personnelles du Client** » désigne les données personnelles traitées par Google au nom du Client dans le cadre de la fourniture par Google des Services de sous-traitance.

« **Incident de données** » désigne une violation de la sécurité de Google entraînant la destruction, perte, modification, divulgation non autorisée ou accès accidentel ou illicite aux Données personnelles du Client sur des systèmes gérés par ou contrôlés par Google. Les « **Incidents de données** » n'incluent pas les tentatives ou

activités infructueuses ne compromettant pas la sécurité des Données personnelles du Client, y compris les tentatives infructueuses de connexion, pings, analyses de port, attaques par déni de service et autres attaques réseau sur pare-feu ou systèmes en réseau.

La « **Législation en matière de protection des données** » désigne, selon le cas : (a) le RGPD ; et/ou (b) la loi fédérale sur la protection des données du 19 juin 1992 (Suisse).

« **Outil mis à la disposition des personnes concernées** » désigne un outil (le cas échéant) mis à disposition par une Entité Google aux personnes concernées permettant à Google de répondre directement et de manière standardisée à certaines demandes des personnes concernées à propos des Données personnelles du Client (par exemple, les paramètres de publicité en ligne ou le plugin du navigateur).

« **EEE** » désigne l'Espace économique européen.

Le « **RGPD** » désigne le Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE.

« **Google** » désigne l'Entité Google qui est partie à l'Accord.

« **Sous-traitants ultérieurs des Sociétés affiliées de Google** » a la signification donnée à la Section 11.1 (Consentement au recours à des sous-traitants ultérieurs).

L'« **Entité Google** » désigne Google LLC (anciennement Google Inc.), Google Ireland Limited ou toute autre Société affiliée de Google LLC.

La « **Certification ISO 27001** » désigne la Certification ISO/IEC 27001:2013 ou une certification comparable pour les Service de sous-traitance

« **Adresse e-mail de notification** » désigne l'adresse e-mail (le cas échéant) choisie par le Client, via l'interface utilisateur des Services de sous-traitance ou tout autre moyen fourni par Google, pour recevoir certaines notifications de Google relatives aux présentes Conditions de traitement des données.

Le « **Privacy Shield** » désigne le cadre juridique de protection des données en vigueur entre l'Union européenne et les-États-Unis, ainsi que le cadre juridique de protection des données en vigueur entre la Suisse et les États-Unis.

« **Services de sous-traitance** » désigne les services en vigueur énumérés sur privacy.google.com/businesses/adsservices.

« **Documentation de sécurité** » désigne le certificat délivré pour la Certification ISO 27001 et toute autre certification ou documentation de sécurité que Google peut mettre à disposition en ce qui concerne les Services de sous-traitance.

« **Mesures de sécurité** » a la signification donnée à la Section 7.1.1 (Mesures de sécurité de Google).

« **Sous-traitants ultérieurs** » désigne les tiers autorisés en vertu des présentes Conditions de traitement des données à avoir un accès logique aux Données personnelles du Client et à les traiter afin de fournir une partie des Services de sous-traitance et tout support technique associé.

« **Durée** » désigne la période allant de la Date d'entrée en vigueur des Conditions jusqu'à la fin de la fourniture par Google des Services de sous-traitance en vertu de l'Accord.

La « **Date d'entrée en vigueur des Conditions** » désigne, le cas échéant :

(a) le 25 mai 2018, si le Client a cliqué pour accepter, ou si les parties ont autrement accepté les présentes Conditions de traitement des données avant ou à cette date ; ou

(b) la date à laquelle le Client a cliqué pour accepter, ou les parties ont autrement accepté les présentes Conditions de traitement des données, si cette date survient après le 25 mai 2018.

« **Sous-traitant ultérieur tiers** » a la signification donnée à la Section 11.1 (Consentement à l'engagement de sous-traitants ultérieurs).

2.2 Les termes « **responsable du traitement** », « **personnes concernées** », « **données personnelles** », « **traitement** », « **sous-traitant** » et « **autorité de contrôle** » tels qu'utilisés dans les présentes Conditions de traitement des données ont les significations données dans le RGPD.

2.3 Toute phrase introduite par les termes « **y compris** », « **comprend** » ou toute expression similaire sera interprétée à titre illustratif et ne limitera pas le sens des mots précédant ces termes. Tout exemple utilisé dans les présentes Conditions de traitement des données n'est fourni qu'à titre illustratif et ne constitue pas le seuls exemple d'un concept donné.

2.4 Toute référence à un cadre juridique, loi ou autre texte législatif est une référence à sa version en vigueur telle que modifiée de temps à autre.

3. Durée des présentes Conditions de traitement des données

Les présentes Conditions de traitement des données prendront effet à la Date d'entrée en vigueur des Conditions et, nonobstant l'expiration de la Durée, resteront en vigueur jusqu'à, et expireront automatiquement dès la suppression de toutes les Données personnelles du Client par Google, comme décrit dans les présentes Conditions de traitement des données.

4. Application des présentes Conditions de traitement des données

4.1 **Application de la Législation en matière de protection des données.** Les présentes Conditions de traitement des données ne s'appliqueront que dans la

mesure où la Législation en matière de protection des données s'applique au traitement des Données personnelles du Client, y compris si :

(a) le traitement s'effectue dans le contexte des activités d'un établissement du Client au sein de l'EEE ; et/ou

(b) les Données personnelles du Client sont des données personnelles relatives à des personnes concernées se trouvant dans l'EEE et le traitement concerne l'offre de biens ou de services ou le suivi de leur comportement au sein de l'EEE.

4.2 **Application aux Services de sous-traitance.** Les présentes Conditions de traitement des données ne s'appliqueront qu'aux Services de sous-traitance pour lesquels les parties ont accepté les présentes Conditions de traitement des données (par exemple : (a) les Services de sous-traitance pour lesquels le Client a cliqué pour accepter les présentes Conditions de traitement des données ou (b) si l'Accord incorpore les présentes Conditions de traitement des données par référence, les Services de sous-traitance qui font l'objet de l'Accord).

5. Traitement des données

5.1 **Rôles et conformité réglementaire; Autorisation.**

5.1.1 **Responsabilités du Sous-traitant et du Responsable du Traitement.** Les parties reconnaissent et conviennent que :

(a) L'Annexe 1 décrit l'objet et les détails du traitement des Données personnelles du Client ;

(b) Google est sous-traitant des Données personnelles du Client conformément à la Législation en matière de protection des données ;

(c) Le Client est responsable du traitement ou sous-traitant, le cas échéant, des Données personnelles du Client conformément à la Législation en matière de protection des données ; et

(d) chaque partie se conformera aux obligations qui lui sont applicables conformément à la Législation en matière de protection des données concernant le traitement des Données personnelles du Client.

5.1.2 **Autorisation par un responsable du traitement tiers.** Si le Client est un sous-traitant, le Client garantit à Google que les consignes et les actions du Client concernant les Données personnelles du Client, y compris sa nomination par Google en tant qu'autre sous-traitant, ont été autorisées par le responsable du traitement compétent.

5.2 **Consignes du Client.** En signant les présentes Conditions de traitement des données, le Client demande à Google de traiter les Données personnelles du Client uniquement conformément à la loi applicable : (a) pour fournir les Services de sous-traitance et tout support technique associé ; (b) tel que précisé plus en détail par l'utilisation par le Client des Services de sous-traitance (y compris dans les

paramètres et autres fonctionnalités des Services de sous-traitance) et tout support technique associé ; (c) tel que documenté sous la forme de l'Accord, y compris les présentes Conditions de traitement des données ; et (d) tel que documenté plus en détail dans d'autres consignes écrites données par le Client et reconnues par Google comme constituant des consignes aux fins des présentes Conditions de traitement des données.

5.3 **Respect des consignes par Google.** Google se conformera aux consignes décrites dans la Section 5.2 (Consignes du Client) (y compris en ce qui concerne les transferts de données), sauf si la législation de l'UE ou d'un État membre de l'UE à laquelle Google est soumise requiert un autre traitement des Données personnelles du Client par Google, auquel cas, Google en informera le Client (sauf si cette loi interdit à Google de le faire pour des motifs importants d'intérêt public).

5.4 **Produits supplémentaires.** Si le Client utilise tout Produit supplémentaire, les Services de sous-traitance peuvent permettre à ces Produits supplémentaires d'accéder aux Données personnelles du Client comme le requiert l'interopérabilité de ces Produits supplémentaires avec les Services de sous-traitance. À des fins de clarté, les présentes Conditions de traitement des données ne s'appliquent pas au traitement des données personnelles en relation avec la fourniture de tout Produit supplémentaire utilisé par le Client, y compris les données personnelles transmises vers ou à partir de ce Produit supplémentaire.

6. Suppression des données

6.1 **Suppression pendant la Durée.**

6.1.1 **Services de sous-traitance avec fonctionnalité de suppression.** Pendant la Durée, si :

(a) la fonctionnalité des Services de sous-traitance inclut l'option pour le Client de supprimer les Données personnelles du Client ;

(b) le Client utilise les Services de sous-traitance pour supprimer certaines Données personnelles du Client ; et

(c) les Données personnelles du Client supprimées ne peuvent pas être récupérées par le Client (par exemple, à partir de la « corbeille »),

alors Google supprimera lesdites Données personnelles du Client de ses systèmes dès que possible et dans un délai maximum de 180 jours, sauf si la législation de l'UE ou d'un État membre de l'UE exige le stockage.

6.1.2 **Services de sous-traitance sans fonctionnalité de suppression.** Pendant la Durée, si la fonctionnalité des Services de sous-traitance n'inclut pas l'option permettant au Client de supprimer les Données personnelles du Client, Google se conformera donc :

(a) à toute demande raisonnable du Client visant à faciliter cette suppression, dans la mesure du possible, compte tenu de la nature et de la fonctionnalité des Services de sous-traitance et

sauf si la législation de l'UE ou d'un État membre de l'UE exige le stockage ; et

(b) aux pratiques de conservation des données décrites sur www.google.com/policies/technologies/ads.

Google peut facturer des frais (sur la base des coûts raisonnables de Google) pour toute suppression de données en vertu de la Section 6.1.2 (a). Google fournira au Client des informations supplémentaires concernant les frais applicables et la base de leur calcul, avant toute suppression desdites données.

6.2 **Suppression à l'expiration de la Durée.** À l'expiration de la Durée, le Client demande à Google de supprimer toutes les Données personnelles du Client (y compris les copies existantes) des systèmes de Google conformément à la loi applicable. Google se conformera à cette consigne dès que possible et dans un délai maximum de 180 jours, sauf si la législation de l'UE ou d'un État membre de l'UE exige le stockage.

7. Sécurité des données

7.1 **Mesures de sécurité et Assistance sécurité de Google.**

7.1.1 **Les Mesures de sécurité de Google.** Google mettra en œuvre et maintiendra des mesures techniques et organisationnelles adéquates pour protéger les Données personnelles du Client contre une destruction, perte, altération, accès ou divulgation non autorisé, accidentel ou illicite, tel que décrit en Annexe 2 (« **Mesures de sécurité** »). Comme décrit en Annexe 2, les Mesures de sécurité comprennent des mesures pour : (a) crypter des données personnelles ; (b) contribuer à garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de Google ; (c) aider à rétablir l'accès en temps voulu aux données personnelles suite à un incident; et (d) effectuer des tests réguliers d'efficacité. Google peut mettre à jour ou modifier les Mesures de sécurité ponctuellement à condition que ces mises à jour et ces modifications n'entraînent pas la dégradation de la sécurité globale des Services de sous-traitance.

7.1.2 **Conformité en matière de sécurité du Personnel de Google.** Google prendra des mesures appropriées afin d'assurer la conformité aux Mesures de sécurité de ses employés, entrepreneurs et Sous-traitants ultérieurs dans la mesure applicable à l'étendue de leur prestation, notamment en veillant à ce que toutes les personnes autorisées à traiter les Données personnelles du Client se soient engagées à la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

7.1.3 **Assistance sécurité de Google.** Le Client accepte que Google (en tenant compte de la nature du traitement des Données personnelles du Client et des informations disponibles pour Google) aide le Client à assurer le respect des obligations du Client en ce qui concerne la sécurité des données personnelles et les violations des données personnelles, y

compris (le cas échéant) les obligations du Client en vertu des Articles 32 à 34 (inclus) du RGPD, en :

(a) mettant en œuvre et en maintenant des Mesures de sécurité conformément à la Section 7.1.1 (Mesures de sécurité de Google) ;

(b) respectant les conditions de la Section 7.2 (Incidents de données) ; et

(c) fournissant au Client la Documentation de sécurité conformément à la Section 7.5.1 (Examens de la documentation de sécurité) et les informations contenues dans les présentes Conditions de traitement des données.

7.2 **Incidents de données.**

7.2.1 **Notification d'incident.** Si Google prend connaissance d'un Incident de données, Google : (a) informera le Client de l'Incident de données rapidement et sans retard injustifié ; et (b) prendra rapidement des mesures raisonnables pour minimiser les dommages et sécuriser les Données personnelles du Client.

7.2.2 **Détails de l'Incident de données.** Les notifications faites conformément à la Section 7.2.1 (Notification d'incident) décriront, dans la mesure du possible, les détails de l'Incident de données, y compris les mesures prises pour atténuer les risques potentiels et les mesures que Google recommande au Client de prendre pour traiter l'Incident de données.

7.2.3 **Livraison de notification.** Google livrera ses notifications de tout Incident de données à l'Adresse e-mail de notification fournie par le Client ou, à la discrétion de Google (y compris si le Client n'a pas fourni une Adresse e-mail de notification), par un autre moyen de communication (par exemple, par appel téléphonique ou via une rencontre en personne). Le Client est seul responsable de fournir l'Adresse e-mail de notification et de s'assurer que l'Adresse e-mail de notification est à jour et valide.

7.2.4 **Notifications des tiers.** Le Client est seul responsable du respect des lois de notification d'incident applicables au Client et de l'exécution des obligations de notification de tiers relatives à tout Incident de données.

7.2.5 **Absence de reconnaissance de faute par Google.** La notification par Google de, ou sa réponse à, un Incident de données conformément à la présente Section 7.2 (Incidents de données) ne sera pas interprétée comme une reconnaissance par Google d'un manquement ou d'une responsabilité en ce qui concerne l'Incident de données.

7.3 **Responsabilités et Évaluation de la sécurité du Client.**

7.3.1 **Responsabilités de la sécurité du Client.** Le Client convient que, sans préjudice des obligations de Google en vertu des Sections 7.1 (Mesures de sécurité et Assistance sécurité de Google) et 7.2 (Incidents de données) :

(a) le Client est seul responsable de son utilisation des Services de sous-traitance, y compris :

(i) en faisant un usage approprié des Services de sous-traitance afin d'assurer un niveau de sécurité approprié au risque en ce qui concerne les Données personnelles du Client ; et

(ii) en sécurisant les informations d'identification, les systèmes et les dispositifs d'authentification du compte que le Client utilise pour accéder aux Services de sous-traitance ; et

(b) Google n'a aucune obligation de protéger les Données personnelles du Client que le client choisit de stocker ou de transférer hors des systèmes de Google et de ses sous-traitants ultérieurs.

7.3.2 **Évaluation de la sécurité du Client.** Le Client reconnaît et accepte que (compte tenu de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement des Données personnelles du Client ainsi que des risques pour les personnes) les Mesures de sécurité mises en œuvre et maintenues par Google, telles qu'énoncées à la Section 7.1.1 (Mesures de sécurité de Google), offrent un niveau de sécurité approprié au risque en ce qui concerne les Données personnelles du Client.

7.4 **Certification de sécurité.** Afin d'évaluer et de garantir l'efficacité continue des Mesures de sécurité, Google conservera la Certification ISO 27001.

7.5 **Examens et Audits de conformité.**

7.5.1 **Examens de la Documentation de sécurité.** Pour démontrer la conformité de Google à ses obligations conformément aux présentes Conditions de traitement des données, Google mettra la Documentation de sécurité à la disposition du Client pour évaluation.

7.5.2 **Droits d'audit du Client.**

(a) Google autorisera le Client ou un vérificateur tiers désigné par le Client à effectuer des audits (y compris des inspections) afin de vérifier la conformité de Google à ses obligations en vertu des présentes Conditions de traitement des données conformément à la Section 7.5.3 (Conditions commerciales supplémentaires pour les audits). Google contribuera auxdits audits tel que décrit à la Section 7.4 (Certification de sécurité) et à la Section 7.5 (Examens et Audits de Conformité).

(b) Le Client peut également effectuer un audit afin de vérifier que Google respecte ses obligations en vertu des présentes Conditions de traitement des données en examinant le certificat délivré pour la Certification ISO 27001 (qui reflète le résultat d'un audit mené par un vérificateur tiers).

7.5.3 **Conditions commerciales supplémentaires pour les audits.**

(a) Le Client enverra à Google toute demande d'audit en application de la Section 7.5.2(a), via les moyens décrits à la Section 12.1 (Contacter Google).

(b) Après réception par Google d'une demande en vertu de la Section 7.5.3(a), Google et le Client discuteront et s'entendront à l'avance sur la date de début raisonnable, la portée et la durée de, et les contrôles de sécurité et de confidentialité applicables à tout audit conformément à la section 7.5.2(a).

(c) Google peut facturer des frais (sur la bases des coûts raisonnables de Google) pour tout audit en application la section 7.5.2(a). Google fournira au Client des informations plus détaillées concernant tout frais applicable et la base de leur calcul, avant un tel audit. Le Client sera responsable de tous les frais facturés par tout vérificateur tiers nommé par le Client pour exécuter un tel audit.

(d) Google peut s'opposer à tout vérificateur tiers nommé par le Client pour effectuer un audit en vertu de la Section 7.5.2(a) si le vérificateur, de l'avis raisonnable de Google, n'a pas les qualifications appropriées ou n'est pas indépendant, est un concurrent de Google ou est autrement inapproprié de manière flagrante. Toute objection de ce type de la part de Google obligera le Client à nommer un autre vérificateur ou à mener l'audit lui-même.

(e) Aucune des présentes Conditions de traitement des données n'impose à Google de divulguer au Client ou à son vérificateur tiers, ou d'autoriser le Client ou son vérificateur tiers à accéder à :

(i) toute donnée de tout autre client d'une Entité Google ;

(ii) toute information comptable ou financière interne de toute Entité Google ;

(iii) tout secret commercial d'une Entité Google ;

(iv) toute information qui, selon l'opinion raisonnable de Google, pourrait : (A) compromettre la sécurité des systèmes ou locaux de l'Entité Google ; ou (B) être la cause de la violation par toute Entité Google de ses obligations en vertu de la Législation en matière de protection des données ou de ses obligations en matière de sécurité et/ou de confidentialité envers le Client ou un tiers ; ou

(v) toute information à laquelle le Client ou son vérificateur tiers cherche à accéder pour toute raison autre que la réalisation en toute bonne foi des

obligations du Client en vertu de la Législation en matière de protection des données.

8. Analyses d'impact et Consultations

Le Client accepte que Google (en tenant compte de la nature du traitement et des informations disponibles pour Google) aide le Client à respecter les obligations du Client en ce qui concerne les analyses d'impact relatives à la protection des données et les consultations préalables, y compris (le cas échéant) les obligations du Client conformément aux Articles 35 et 36 du RGPD, en :

(a) fournissant la Documentation de sécurité conformément à la Section 7.5.1 (Examens de la Documentation de sécurité) ;

(b) fournissant les informations contenues dans les présentes Conditions de traitement des données ; et en

(c) fournissant ou en mettant autrement à disposition, conformément aux pratiques standard de Google, d'autres documents concernant la nature des Services de sous-traitance et le traitement des Données personnelles du Client (par exemple, les documents du centre d'aide).

9. Droits des personnes concernées par ces données

9.1 **Réponses aux demandes des personnes concernées par ces données.** Si Google reçoit une demande d'une personne concernée par ces données relative aux Données personnelles du Client, Google :

(a) si la demande est effectuée via un Outil mis à la disposition des personnes concernées, répondra directement à la demande de la personne concernée conformément à la fonctionnalité standard de cet Outil mis à la disposition des personnes concernées ; ou

(b) si la demande n'est pas faite via un Outil mis à la disposition des personnes concernées, conseillera à la personne concernée de soumettre sa demande au Client, et le Client sera alors responsable de répondre à une telle demande.

9.2 **Assistance apportée par Google relative aux demandes des personnes concernées.** Le Client convient que Google (en tenant compte de la nature du traitement des Données personnelles du Client et, le cas échéant, de l'Article 11 du RGPD) aide le Client à satisfaire toute obligation de répondre aux demandes des personnes concernées, y compris (le cas échéant) l'obligation du Client de répondre aux demandes d'exercice des droits des personnes concernées, énoncées au Chapitre III du RGPD, en :

(a) fournissant la fonctionnalité des Services de sous-traitance ;

(b) respectant les engagements énoncés à la Section 9.1 (Réponses aux demandes des personnes concernées) ; et

(c) si applicable aux Services de sous-traitance, mettant à disposition des Outils spécifiques aux personnes concernées.

10. Transferts de données

10.1 **Stockage des données et sites de traitement.** Le Client convient que Google peut, sous réserve de la Section 10.2 (Transferts de données hors de l'EEE et de la Suisse), stocker et traiter les Données personnelles du Client aux États-Unis d'Amérique ou dans tout autre pays où Google ou l'un de ses sous-traitants ultérieurs ont un site.

10.2 **Transferts de données hors de l'EEE et de la Suisse.** Google s'assurera que :

(a) la société mère du groupe Google, Google LLC, demeure auto-certifiée conformément au "Privacy Shield" pour son compte et celui de ses filiales américaines en propriété exclusive ; et

(b) la portée de la certification au "Privacy Shield" de Google LLC comprend les Données personnelles du Client.

10.3 **Informations relatives aux centres de données.** Les informations concernant la localisation des centres de données de Google sont disponibles sur www.google.com/about/datacenters/inside/locations/index.html.

11. Sous-traitants ultérieurs

11.1 **Consentement à l'engagement de Sous-traitants ultérieurs.** Le client autorise spécifiquement l'engagement des Sociétés affiliées de Google en tant que Sous-traitants ultérieurs (« **Sociétés affiliées sous-traitants ultérieurs de Google** »). En outre, le Client autorise de manière générale l'engagement de tout tiers en tant que Sous-traitant ultérieur (« **Sous-traitant ultérieur tiers** »).

11.2 **Informations concernant les Sous-traitants ultérieurs.** Les informations concernant les Sous-traitants ultérieurs sont disponibles sur privacy.google.com/businesses/subprocessors.

11.3 **Exigences relatives au recours à des Sous-traitants ultérieurs.** En ayant recours à un Sous-traitant ultérieur, Google :

(a) s'assure via un accord écrit que :

(i) le Sous-traitant ultérieur accède à et utilise uniquement les Données personnelles du Client dans la mesure requise pour exécuter les obligations qui lui sont sous-traitées, et le fait conformément à l'Accord (y compris les présentes Conditions de traitement des données) et au "Privacy Shield" ; et

(ii) si le RGPD s'applique au traitement des Données personnelles du Client, les obligations de protection des données énoncées à l'Article 28(3) du RGPD sont imposées au Sous-traitant ultérieur ; et

(b) demeure responsable de toutes les obligations sous-traitées et de l'ensemble des actes ou des omissions de ses Sous-traitants ultérieurs.

11.4 **Possibilité d'opposition aux changements de Sous-traitants ultérieurs.**

(a) Lorsqu'un nouveau Sous-traitant ultérieur tiers est engagé pendant la Durée, Google, au moins 30 jours avant que le nouveau Sous-traitant ultérieur tiers traite les Données personnelles du Client, informe le Client de l'engagement (y compris le nom et le lieu du Sous-traitant ultérieur concerné et les activités qu'il effectuera) en envoyant un e-mail à l'Adresse e-mail de notification.

(b) Le Client peut s'opposer à tout nouveau Sous-traitant ultérieur tiers en résiliant l'Accord immédiatement suivant notification écrite à Google, à condition que le Client fournisse une telle notification dans les 90 jours après avoir été informé de l'engagement du nouveau Sous-traitant ultérieur tiers tel que décrit à la Section 11.4(a). Ce droit de résiliation est le seul et unique recours du Client si le Client s'oppose à tout nouveau Sous-traitant ultérieur tiers.

12. Contacter Google; Registre des Traitements

12.1 **Contacter Google.** Le Client peut contacter Google concernant l'exercice de ses droits conformément aux présentes Conditions de traitement des données via les méthodes décrites sur privacy.google.com/businesses/processorsupport ou via d'autres moyens fournis par Google ponctuellement.

12.2 **Registre des Traitements de Google.** Le Client reconnaît que Google est tenu par le RGPD de : (a) recueillir et tenir à jour certaines informations, y compris le nom et les coordonnées de chaque sous-traitant et/ou responsable du traitement pour le compte duquel Google agit et (le cas échéant) du représentant local et du délégué à la protection des données dudit sous-traitant ou responsable du traitement ; et (b) mettre ces informations à la disposition des autorités de contrôle. En conséquence, le Client, sur demande et le cas échéant, fournira de telles informations à Google via l'interface utilisateur des Services de sous-traitance ou par tout autre moyen fourni par Google, et utilisera cette interface utilisateur ou d'autres moyens pour garantir que toutes les informations fournies sont exactes et à jour.

13. Responsabilité

Si l'Accord est régi par les lois :

(a) d'un État des États-Unis d'Amérique, alors, nonobstant tout ce qui figure dans l'Accord, la responsabilité totale de l'une des parties vis-à-vis de l'autre partie dans le cadre ou en relation avec les présentes Conditions de traitement des données sera limitée à la valeur monétaire ou au paiement maximum auquel la responsabilité de cette partie est plafonnée en vertu de l'Accord (par souci de clarté, toute exclusion de demande d'indemnisation issue de toute clause limitative de responsabilité de l'Accord ne sera pas applicable aux demandes

d'indemnisations faites en application de l'Accord et relatives à la Législation en matière de protection des données) ; ou

(b) d'une juridiction qui n'est pas un État des États-Unis d'Amérique, alors la responsabilité des parties dans le cadre ou en relation avec les présentes Conditions de traitement des données sera soumise aux exclusions et aux limitations de responsabilité figurant dans l'Accord.

14. Effet des présentes Conditions de traitement des données

En cas de conflit ou d'incohérence entre les présentes Conditions de traitement des données et le reste de l'Accord, ce sont les présentes Conditions de traitement des données qui prévaudront. Sous réserve des amendements contenus dans les présentes Conditions de traitement des données, l'Accord reste pleinement en vigueur.

15. Modifications des présentes Conditions de traitement des données

15.1 **Modifications des URLs.** Google peut ponctuellement modifier toute URL référencée dans les présentes Conditions de traitement des données et le contenu de ces URL. Google peut uniquement modifier la liste des potentiels Services de sous-traitance sur privacy.google.com/businesses/adsservices:

(a) pour refléter un changement dans le nom d'un service ;

(b) pour ajouter un nouveau service ; ou

(c) pour retirer un service lorsque soit : (i) tous les contrats relatifs à la fourniture de ce service sont résiliés ; ou (ii) Google a le consentement du Client.

15.2 **Modifications des Conditions de traitement des données.** Google peut modifier les présentes Conditions de traitement des données si la modification :

(a) est expressément autorisée par les présentes Conditions de traitement des données, y compris celles décrites à la Section 15.1 (Modifications des URLs) ;

(b) reflète une modification dans le nom ou la forme d'une entité juridique ;

(c) est nécessaire pour se conformer au droit applicable, à la réglementation, à une ordonnance judiciaire ou règle applicable émise par un organisme de réglementation ou une administration gouvernementale ; ou

(d) (i) ne résulte pas d'une dégradation de la sécurité globale des Services de sous-traitance ; (ii) n'étend pas la portée, ou ne supprime pas toute restriction, du traitement des Données personnelles du Client par Google, comme décrit à la Section 5.3 (Conformité de Google aux consignes) ; et (iii) n'a pas d'autre impact négatif important sur les droits du Client dans

le cadre des présentes Conditions de traitement des données, tel que raisonnablement déterminé par Google.

15.3 **Notification de modifications.** Si Google a l'intention de modifier les présentes Conditions de traitement des données conformément à la Section 15.2(c) ou (d), Google informera le Client au moins 30 jours (ou toute période plus courte requise pour se conformer à la loi applicable, à la réglementation applicable, à une ordonnance judiciaire ou à une directive émise par un organisme de réglementation ou une administration gouvernementale) avant que le changement ne prenne effet en : (a) envoyant un e-mail à l'Adresse e-mail de notification ; ou (b) alertant le Client via l'interface utilisateur pour les Services de sous-traitance. Si le Client s'oppose à une telle modification, le Client peut résilier l'Accord en envoyant un avis écrit à Google dans les 90 jours suivant la notification du changement par Google.

Annexe 1 : Objet et détails du Traitement des données

Objet

La fourniture par Google des Services de sous-traitance et de toute assistance technique associée au Client.

Durée du Traitement

La Durée plus la période à compter de l'expiration de la Durée jusqu'à la suppression de toutes les Données personnelles du Client par Google conformément aux présentes Conditions de traitement des données.

Nature et fins du Traitement

Google traitera (y compris, en ce qui concerne les Services de sous-traitance et les consignes décrites à la Section 5.2 (Consignes du Client), le recueil, l'enregistrement, l'organisation, la structuration, le stockage, la modification, l'extraction, l'utilisation, la divulgation, la combinaison et l'effacement) les Données personnelles du Client aux fins de fournir les Services de sous-traitance et toute assistance technique au Client conformément aux présentes Conditions de traitement des données.

Types de Données personnelles

Les données personnelles du Client peuvent inclure les types de données personnelles décrites sur privacy.google.com/businesses/adsservices.

Catégories des personnes concernées

Les Données personnelles du Client concerneront les catégories suivantes de personnes concernées :

- les personnes concernées au sujet desquelles Google recueille des données personnelles dans le cadre de la fourniture des Services de sous-traitance ; et/ou
- les personnes concernées au sujet desquelles des données personnelles sont transférées à Google concernant les Services de sous-traitance par, sous la direction de, ou au nom du Client.

Selon la nature des Services de sous-traitance, ces personnes concernées peuvent inclure des personnes : (a) à qui la publicité en ligne a été ou sera adressée ; (b) qui ont visité des sites Internet ou des applications spécifiques pour lesquels Google fournit les services de sous-traitance ; et/ou (c) qui sont des clients ou des utilisateurs des produits ou services du Client.

Annexe 2 : Mesures de sécurité

À compter de la date d'entrée en vigueur des Conditions, Google mettra en œuvre et maintiendra les Mesures de sécurité énoncées dans la présente Annexe 2. Google peut mettre à jour ou modifier ces Mesures de sécurité ponctuellement à condition que ces mises à jour et ces modifications n'entraînent pas la dégradation de la sécurité globale des Services de sous-traitance.

1. Centre de données et Sécurité du réseau

(a) **Centres de données.**

Infrastructure. Google gère des centres de données répartis dans différentes zones géographiques. Google stocke l'ensemble des données de production dans des centres de données physiquement sécurisés.

Redondance. Les systèmes d'infrastructure ont été conçus pour éliminer les points de panne uniques et réduire l'impact des risques environnementaux prévisibles. Les circuits doubles, les interrupteurs, les réseaux et autres appareils nécessaires contribuent à fournir cette redondance. Les Services de sous-traitance sont conçus pour permettre à Google de réaliser certains types de maintenance préventive et corrective sans interruption. Tous les équipements et installations environnementaux ont des procédures de maintenance préventives documentées qui détaillent le processus permettant la performance, ainsi que sa fréquence, conformément aux spécifications internes ou à celles du fabricant. La maintenance préventive et corrective des équipements du centre de données est programmée via un processus de traitement standard basé sur des procédures documentées.

Alimentation. Les systèmes électriques du centre de données sont conçus pour être redondants et susceptibles de subir une maintenance sans impact sur les opérations continues, 24h/24 et 7j/7. Dans la plupart des cas, une source d'alimentation principale, ainsi qu'une source alternative, chacune de capacité égale, sont fournies pour les composants d'infrastructure importants au sein du centre de données. Une alimentation électrique de secours est fournie par divers mécanismes comme des batteries d'alimentation électrique ininterruptibles (uninterruptible power supply, UPS), qui fournissent une protection électrique fiable à tout instant, pendant les baisses de tension, les pannes d'électricité, les surtensions, les sous-tensions et les conditions de fréquence situées en dehors des zones de tolérance du système. Si le courant fourni par le réseau collectif est interrompu, l'alimentation électrique de secours est conçue pour fournir un courant

transitoire au centre de données, à pleine capacité, pour une durée allant jusqu'à 10 minutes, le temps que les systèmes de générateurs au diesel prennent le relais. Les générateurs au diesel sont en mesure de s'enclencher automatiquement en quelques secondes pour fournir suffisamment de courant électrique de secours pour alimenter le centre de données à pleine capacité sur plusieurs jours.

Systèmes d'exploitation des serveurs. Les serveurs Google utilisent des systèmes d'exploitation renforcés, personnalisés pour les besoins uniques de l'entreprise en matière de serveur. Les données sont stockées à l'aide d'algorithmes exclusifs pour renforcer la sécurité et la redondance des données. Google utilise un processus d'examen de code pour accroître la sécurité du code utilisé pour fournir les Services de sous-traitance et améliorer les produits de sécurité dans les environnements de production.

Continuité des activités. Google réplique les données sur plusieurs systèmes pour aider à se prémunir contre les destructions ou pertes accidentelles. Google a conçu ses programmes de planification de la continuité des activités/de récupération après sinistre. En outre, il les planifie et les teste de façon régulière.

(b) **Réseaux et transmission.**

Transmission des données. Les centres de données sont généralement connectés via des liens privés à grande vitesse afin de fournir des transferts de données sûrs et rapides entre les centres de données. Ce dispositif vise à empêcher que les données ne soient lues, copiées, altérées ou retirées sans autorisation pendant le transfert ou le transport électronique, ou pendant leur enregistrement sur des médias de stockage de données. Google transfert les données via des protocoles Internet standard.

Surface d'attaque externe. Google utilise plusieurs couches d'appareils en réseau et de détection des intrusions pour protéger sa surface d'attaque externe. Google considère les vecteurs potentiels d'attaque et incorpore des technologies spécifiquement conçues dans les systèmes en contact avec l'extérieur.

Détection des intrusions. La détection des intrusions vise à fournir des données sur les activités d'attaque continues et des informations adéquates pour réagir aux incidents. La détection des intrusions de Google implique :

1. Un contrôle étroit de la taille et de la composition de la surface d'attaque de Google via des mesures préventives ;

2. L'utilisation de contrôles de détection intelligents au niveau des points d'entrée des données ; et

3. L'utilisation de technologies qui pallient automatiquement à certaines situations dangereuses.

Réaction aux incidents. Google assure le suivi de divers canaux de communication pour les incidents de sécurité, et le personnel de sécurité de Google réagira rapidement aux incidents connus.

Technologies de cryptage. Google met à disposition un cryptage HTTPS (aussi connu sous le nom de connexion SSL ou TLS). Les serveurs de Google supportent

l'échange de clé cryptographique Diffie Hellman basé sur la courbe elliptique éphémère signé avec RSA et ECDSA. Ces méthodes de confidentialité persistante parfaites (perfect forward secrecy, PFS) permettent de protéger le trafic et de minimiser l'impact d'une clé corrompue ou d'une rupture dans la cryptographie.

2. Accès et contrôles du site

(a) **Contrôles du site.**

Dispositif de sécurité du centre de données sur site. Les centres de données de Google gèrent un dispositif de sécurité sur site responsable de l'ensemble des fonctions de sécurité physique des centres de données 24h/24, 7j/7. Le personnel en charge du dispositif de sécurité sur site assure le suivi des caméras de surveillance (« **CCTV** ») et de l'ensemble des systèmes d'alarme. Le personnel en charge du dispositif de sécurité sur site réalise régulièrement des patrouilles internes et externes au niveau du centre de données.

Procédures d'accès au centre de données. Google a mis en place des procédures d'accès formelles pour permettre l'accès physique aux centres de données. Les centres de données sont hébergés dans des installations qui nécessitent un accès via un badge électronique, avec des alarmes reliées au dispositif de sécurité sur site. Toutes les personnes qui pénètrent dans le centre de données doivent s'identifier et présenter un justificatif d'identité au dispositif de sécurité sur site. Seuls les employés, les prestataires et les visiteurs autorisés peuvent entrer dans les centres de données. Seuls les employés et prestataires autorisés sont autorisés à demander un accès par badge électronique à ces installations Les demandes d'accès par de badge électronique aux centres de données doivent être effectuées à l'avance par écrit, et nécessitent l'approbation du responsable hiérarchique du demandeur et du directeur du centre de données. Tous les autres visiteurs qui demandent un accès temporaire au centre de données doivent : (i) obtenir une approbation à l'avance des responsables du centre de données pour le site de données en question et les zones internes qu'ils souhaitent visiter ; (ii) s'identifier auprès du dispositif de sécurité sur site ; et (iii) apporter une preuve d'accès à un centre de données identifiant la personne comme étant approuvée.

Appareils de sécurité du centre de données sur site. Les centres de données de Google utilisent un accès par badge électronique et un système de contrôle d'accès biométrique relié à un système d'alarme. Le système de contrôle d'accès surveille et enregistre l'ensemble des badges électroniques, y compris lorsque les personnes accèdent aux portes extérieures, lorsque des colis sont expédiés ou réceptionnés, et à d'autres endroits stratégiques. Les activités non autorisées et les tentatives d'accès infructueuses sont consignées par le système de contrôle d'accès et étudiées, le cas échéant. L'accès autorisé sur l'ensemble du dispositif commercial et des centres de données est restreint par zones et dépend des responsabilités liées aux fonctions de chacun. Les portes coupe-feu des centres de données sont équipées d'alarmes. Les caméras de surveillance fonctionnent à l'intérieur comme à l'extérieur des centres de données. Le positionnement des caméras a été conçu pour couvrir des zones stratégiques, y compris, entre autres, le périmètre, les portes d'accès au bâtiment du centre de données, et les zones d'expédition et de réception. Le personnel du dispositif de sécurité sur site gère le

suivi, l'enregistrement et le contrôle des équipements du dispositif de surveillance par caméras. Des câbles sécurisés parcourant les centres de données connectent les équipements du dispositif de surveillance par caméras. Les caméras effectuent un enregistrement sur site à l'aide d'enregistreurs vidéo 24h/24 et 7j/7. Les enregistrements de surveillance sont conservés au moins 7 jours en fonction de l'activité.

(b) **Contrôle de l'accès.**

Personnel en charge de la sécurité de l'infrastructure. Google dispose et entretient une politique de sécurité à l'intention de son personnel, et exige de ses employés qu'ils suivent une formation en matière de sécurité dans le cadre du dispositif de formation qui leur est destiné. Le personnel de Google en charge de la sécurité de l'infrastructure est responsable de la surveillance continue de la sécurité de l'infrastructure de Google, de l'examen des Services de sous-traitance, et est tenu de réagir en cas d'incidents de sécurité.

Contrôle d'accès et gestion des privilèges. Les administrateurs du Client et les utilisateurs doivent s'identifier via un système d'identification central ou via un système de connexion unique afin d'utiliser les Services de sous-traitance.

Processus et politiques internes d'accès aux données : Politique d'accès. Les processus et politiques internes d'accès aux données de Google sont conçus pour empêcher des personnes et/ou des systèmes non autorisés d'obtenir un accès aux systèmes utilisés pour le traitement des données personnelles. Google s'efforce de concevoir ses système en vue de : (i) permettre uniquement aux personnes autorisées d'accéder aux données pour lesquelles elles possèdent une autorisation ; (ii) veiller à ce que les données personnelles ne soient pas lues, copiées, altérées ou retirées sans autorisation pendant leur traitement, leur utilisation et après leur enregistrement. Les systèmes sont conçus pour détecter tout accès inapproprié. Google utilise un système de gestion d'accès centralisé pour contrôler l'accès du personnel aux serveurs de production, et fournit uniquement un accès à un nombre limité d'employés autorisés. LDAP, Kerberos et un système exclusif utilisant des certificats SSH sont conçus pour fournir à Google des mécanismes d'accès sûrs et flexibles. Ces mécanismes sont conçus pour octroyer uniquement des droits d'accès autorisés aux hébergeurs de site, aux journaux de connexion, aux données et aux informations de configuration. Google requiert l'utilisation d'identifiants utilisateur uniques, de mots de passe puissants, d'une identification à deux facteurs et de listes d'accès soigneusement contrôlées pour réduire les possibilités d'utilisation non autorisée de comptes. L'octroi ou la modification des droits d'accès dépendent : des responsabilités professionnelles du personnel autorisé ; des exigences professionnelles nécessaires pour réaliser les tâches autorisées ; et de la nécessité de l'accès. L'octroi ou la modification des droits d'accès doivent également être conformes aux politiques et aux formations internes de Google relatives à l'accès aux données. Les approbations sont gérées par des outils de flux de travail qui mettent à jour les dossiers d'audit en prenant en compte toutes les modifications. L'accès aux systèmes est consigné pour créer une trace d'audit permettant la responsabilité. Là où des mots de passe sont utilisés à des fins d'identification (p. ex., la connexion aux stations de travail), des politiques de mot de passe respectant au minimum les normes du secteur sont mises en œuvre. Ces

normes comprennent des restrictions à la réutilisation du mot de passe et des niveaux de puissance suffisants pour les mots de passe.

3. Données

(a) **Stockage, isolation et authentification des données.**

Google stocke des données dans un environnement multi-tenant sur des serveurs dont Google a la propriété. Les données, la base de données des Services de sous-traitance et l'architecture du système de fichiers sont reproduites dans plusieurs centres de données répartis sur plusieurs zones géographiques. Google isole logiquement les données de chaque client. Un système d'identification central est utilisé pour tous les Services de sous-traitance afin d'accroître la sécurité uniforme des données.

(b) **Consignes sur les Disques mis hors service et la suppression des disques.**

Certains disques contenant des données peuvent rencontrer des problèmes de performance, des erreurs ou des défaillances matérielles entraînant leur mise hors service (« **Disque mis hors service** »). Chaque Disque mis hors service est soumis à une série de processus de destruction des données (les « **Consignes de suppression des Données** ») avant de quitter les sites de Google pour être réutilisé ou détruit. Les Disques mis hors service sont effacés selon un processus à plusieurs étapes dont la complétude est vérifiée par au moins deux personnes indépendantes en charge de la validation du processus. Les résultats de l'effacement sont consignés avec le numéro de série du Disque mis hors service pour suivi. Enfin, le Disque mis hors service et effacé est acheminé au stock pour réutilisation et redéploiement. Si, en raison d'une défaillance matérielle, le Disque mis hors service ne peut être effacé, il est stocké de façon sécurisée jusqu'à sa destruction. Chaque installation fait l'objet d'un audit régulier afin de contrôler la conformité aux Consignes de suppression des Données.

4. Sécurité du personnel.

Le personnel de Google doit se comporter d'une manière conforme aux directives de la société en matière de confidentialité, de déontologie, d'utilisation appropriée et de normes professionnelles. Google mène des vérifications d'antécédents adéquates et raisonnables dans la limite définie par la loi et conformément à la législation du travail et aux textes légaux du pays concerné.

Le personnel est tenu de signer un accord de confidentialité et doit accuser réception des politiques de confidentialité et de respect de la vie privée de Google, et reconnaître y adhérer. Le personnel reçoit une formation sur la sécurité. Le personnel en charge des Données personnelles du Client est tenu de se conformer aux exigences supplémentaires liées à sa fonction. Le personnel de Google ne traitera aucune des Données personnelles du Client sans autorisation.

5. Sécurité des Sous-traitants ultérieurs

Avant de collaborer avec des Sous-traitants ultérieurs, Google mène un audit de leurs pratiques en matière de sécurité et de respect de la vie privée afin de s'assurer que les Sous-traitants ultérieurs fournissent un niveau de sécurité et de respect de la vie privée approprié à leur accès aux données et à la portée des services pour lesquels ils ont été engagés. Une fois que Google a évalué les risques que présente le Sous-traitant ultérieur, toujours sous réserve des exigences décrites à la Section 11.3 (Exigences relatives au recours à des Sous-traitants ultérieurs), le Sous-traitant ultérieur est tenu de signer des clauses contractuelles adéquates en matière de sécurité, de confidentialité et de respect de la vie privée.

Conditions de traitement des données Google Ads, Version 1.2

12 octobre 2017