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 de certaines données dans le cadre de la Législation Européenne en matière de protection des données et de certaines Législations Non-Européennes en matière de protection des données.

2.Définitions et Interprétation

2.1Dans 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.

« **Conditions Supplémentaires pour la Législation Non-Européenne en matière de protection des données** » désigne les conditions supplémentaires visées à l'Annexe 3, qui reflètent l'accord des parties sur les conditions régissant le traitement de certaines données dans le cadre de certaines Législations Non-Européennes en matière de protection des données.

« **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.

« **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 de l'UE** » 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.

La « **Législation Européenne 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).

« **Législation Européenne ou Nationale** » signifie, selon le cas : (a) la législation de l'UE ou d'un État Membre de l'UE (si le RGPD de l'UE s'applique au traitement de Données personnelles du Client) et/ou (b) la législation du Royaume-Uni ou d'une partie du Royaume-Uni (si le RGPD du Royaume-Uni s'applique au traitement des Données personnelles du Client).

« **RGPD** » signifie, selon le cas : (a) le RGPD de l'UE ; et/ou (b) le RGDP du Royaume-Uni.

« **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.

« **Clauses Contractuelles Types** » signifie les clauses disponibles à l'adresse https://privacy.google.com/businesses/processorterms/mccs, qui sont des clauses standard de protection des données pour le transfert de données personnelles à des sous-traitants établis dans des pays tiers qui n'assurent pas un niveau adéquat de protection des données, comme décrit dans l'article 46 du RGPD de l'UE.

La « **Législation Non-Européenne en matière de protection des données** » désignent les lois en matière de protection des données ou de la vie privée en vigueur en dehors de l'Espace Economique Européen, de la Suisse et du Royaume-Uni.

« **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.

« **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.

« **Autorité de Contrôle** » signifie, selon le cas : (a) une "autorité de contrôle" telle que définie dans le RGPD de l'UE ; et/ou (b) le "Commissioner" tel que défini dans le RGPD du Royaume-Uni.

« **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).

« **RGPD du Royaume-Uni** » signifie le RGPD UE tel qu'amendé et incorporé dans la législation du Royaume-Uni en application du European Union (Withdrawal) Act 2018, si ce dernier est en vigueur.

2.2 Les termes « **responsable du traitement** », « **personnes concernées** », « **données personnelles** », « **traitement** » et « **sous-traitant** » tels qu'utilisés dans les présentes Conditions de traitement des données ont les significations données dans le RGPD, et les termes "importateur de données" et "exportateur de données" ont la signification qui leur est donnée dans les Clauses Contractuelles Types.

2.3 Les termes « **inclure** » et « **y compris** » signifient « **y compris, mais sans limitations** » . 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.

2.5 Si les présentes Conditions de traitement des données sont traduites dans une autre langue et qu'il existe une divergence entre le texte anglais et le texte traduit, le texte anglais fera foi.

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 Européenne en matière de protection des données**. Les sections 5 (Traitement des données) à 12 (Contacter Google ; Registre des Traitements) (inclus) ne s'appliqueront que dans la mesure où la Législation Européenne 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 ou du Royaume-Uni ; et/ou

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

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).

4.3 **Intégration des Conditions Supplémentaires pour la Législation Non-Européenne en matière de protection des données**. Les Conditions Supplémentaires pour la Législation Non-Européenne en matière de protection des données complètent les présentes Conditions de traitement des données.

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 Européenne 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 Européenne en matière de protection des données ; et

(d) chaque partie se conformera aux obligations qui lui sont applicables conformément à la Législation Européenne 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 Européenne ou Nationale 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 législation 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 Européenne ou Nationale 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 Européenne ou Nationale exige le stockage ; et

(b) aux pratiques de conservation des données décrites sur policies.google.com/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 Européenne ou Nationale 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 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) Si les Clauses Contractuelles Type s'appliquent en vertu de la Section 10.2 (Transferts de données), Google autorisera le Client ou un auditeur tiers désigné par le Client à effectuer les audits décrits dans les Clauses Contractuelles Types conformément à la section 7.5.3 (Conditions commerciales supplémentaires pour les Audits).

(c) 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) ou 7.5.2(b), 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) ou 7.5.2(b).

(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) ou 7.5.2(b). 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) ou 7.5.2(b) 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 Européenne 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 Européenne en matière de protection des données.

7.5.4 Pas de modification des Clauses Contractuelles Types. Si les Clauses Contractuelles Types s'appliquent en vertu de la Section 10.2 (Transferts de données), rien dans la présente section 7.5 (Examens et Audits de conformité) ne modifie les droits ou obligations du Client ou de Google LLC en vertu des Clauses Contractuelles Types.

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), stocker et traiter les Données personnelles du Client dans tout pays où Google ou l'un de ses sous-traitants ultérieurs ont un site.

10.2 **Transferts de données.**

Si le stockage et/ou le traitement des Données Personnelles du Client implique des transferts de Données Personnelles du Client de l'EEE, de la Suisse ou du Royaume-Uni vers un pays tiers qui n'est pas soumis à une décision d'adéquation en vertu de la Législation Européenne en matière de protection des données :

(a) Le Client (en tant qu'exportateur de données) sera réputé avoir conclu les Clauses Contractuelles Types avec Google LLC (en tant qu'importateur de données) ;

(b) les transferts seront soumis aux Clauses Contractuelles Types ; et

(c) Google veillera à ce que Google LLC respecte ses obligations au titre de ces Clauses Contractuelles Types en ce qui concerne ces transferts.

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/locations/.

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** »). Si les Clauses Contractuelles Type s'appliquent en vertu de la section 10.2 (Transferts de données), les autorisations ci-dessus constituent le consentement écrit préalable du client à la sous-traitance par Google LLC du traitement des Données personnelles du Client.

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, si elles sont applicables en vertu de la Section 10.2 (Transferts de données), les Clauses Contractuelles Type; 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 de toute Autorité 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

13.1 Plafond de 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 Européenne en matière de protection des données ou à la Législation Non-Européenne 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.

13.2 Responsabilité si les Clauses Contractuelles Types s'appliquent. Si les Clauses Contractuelles Type s'appliquent en vertu de la Section 10.2 (Transferts de données), alors la responsabilité totale combinée de:

(a) Google, Google LLC et Google Ireland Limited envers le Client ; et

(b) Le Client envers Google, Google LLC et Google Ireland Limited,

dans le cadre de l'Accord ou en relation avec celui-ci, et des Clauses Contractuelles Types combinés seront soumis à la Section 13.1 (Plafond de Responsabilité).

14. Tiers Bénéficiaire

Lorsque Google LLC n'est pas partie à l'Accord et que les Clauses Contractuelles Types s'appliquent en vertu de la section 10.2 (Transferts de données), Google LLC sera un tiers bénéficiaire des sections 6.2 (Suppression à l'expiration de la Durée), 7.5 (Examens et Audits de conformité), 9.1 (Réponses aux Demandes des Personnes Concernées), 10.2 (Transferts de données), 11.1 (Consentement à l'engagement de Sous-traitants ultérieurs) et 13.2 (Responsabilité si les Clauses Contractuelles Types s'appliquent). Dans la mesure où la présente Section 14 (Tiers Bénéficiaire) entre en conflit ou est incompatible avec toute autre clause de l'Accord, la présente section 14 (Tiers Bénéficiaire) s'appliquera.

15. Effet des présentes Conditions de traitement des données

En cas de conflit ou d'incohérence entre les Clauses Contractuelles Types, les Conditions Supplémentaires pour la Législation Non-Européenne en matière de protection des données, et le reste des présentes Conditions de traitement des données et/ou le reste de l'Accord, l'ordre de priorité suivant s'applique : (a) les Clauses Contractuelles Types, (b) les Conditions Supplémentaires pour la Législation Non-Européenne en matière de protection des données ; (c) le reste des présentes Conditions de traitement des données ; et (d) le reste de l'Accord. Sous réserve des amendements contenus dans les présentes Conditions de traitement des données, l'Accord reste pleinement en vigueur.

16. Modifications des présentes Conditions de traitement des données

16.1 **Modifications des URLs.** Google peut ponctuellement modifier toute URL référencée dans les présentes Conditions de traitement des données et le contenu de ces URL, à l'exception de ce qui suit:

(a) Google ne peut modifier les Clauses Contractuelles Types que conformément aux sections 16.2(b) - 16.2(d) (Modifications des Conditions de Traitement des Données) ou pour intégrer toute nouvelle version des Clauses Contractuelles Types qui pourrait être adoptée en vertu de la Législation Européenne en matière de protection des données, dans chaque cas d'une manière qui n'affecte pas la validité des Clauses Contractuelles Types en vertu de la Législation Européenne en matière de protection des données ; et

(b) Google peut uniquement modifier la liste des potentiels Services de sous-traitance sur privacy.google.com/businesses/adsservices:

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

(ii) pour ajouter un nouveau service ; ou

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

16.2 **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 16.1 (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, (x) s'agissant des Conditions Supplémentaires pour la Législation Non-Européenne en matière de protection des données, sur les droits de Google d'utiliser ou de traiter les données visées par les Conditions Supplémentaires pour la Législation Non-Européenne en matière de protection des données ou (y) s'agissant du reste de ces Conditions de traitement des données, sur le 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.

16.3 **Notification de modifications.** Si Google a l'intention de modifier les présentes Conditions de traitement des données conformément à la Section 16.2(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 est tenu de mettre en place et de maintenir les Mesures de sécurité définies 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. Sécurité des centres de données et des réseaux

(a) **Centres de données.**

Infrastructure. Google gère des centres de données répartis dans différents endroits. Google stocke toutes les données de production dans des centres de données physiques sécurisés.

Redondance. Les systèmes d'infrastructure ont été conçus de manière à éliminer les points de défaillance uniques et à minimiser l'impact des risques environnementaux anticipés. Cette redondance repose entre autres sur des circuits doubles, des commutateurs, des réseaux et d'autres appareils. Les Services de sous-traitance visent à permettre à Google d'effectuer certains types d'opérations de maintenance préventive et corrective sans interruption. L'ensemble des installations et des équipements environnementaux sont associés à des procédures de maintenance préventive documentées, qui détaillent le processus et la fréquence d'intervention en fonction des spécifications du fabricant ou des spécifications internes. La maintenance préventive et corrective de l'équipement des centres de données est planifiée en suivant un processus standard respectant des procédures documentées.

Alimentation. Les systèmes électriques des centres de données sont conçus pour être redondants et de sorte que leur maintenance puisse être assurée sans interrompre leur fonctionnement continu (24h/24, 7j/7). Dans la plupart des cas, les composants d'infrastructure essentiels des centres de données présentent une source d'alimentation principale et une source d'alimentation secondaire (de capacité égale). L'alimentation de secours est assurée par différents mécanismes tels que des batteries d'alimentation sans interruption. Les systèmes de ce type permettent de fournir en continu une protection fiable de l'alimentation en cas de baisse de tension, de panne, de surtension, de sous-tension et de fréquence hors tolérance au niveau du circuit. En cas d'interruption de l'alimentation, le réseau de secours est censé alimenter le centre de données de façon transitoire, à pleine capacité, pendant 10 minutes maximum, jusqu'à ce que les générateurs diesel prennent le relais. Les générateurs diesel sont capables de démarrer automatiquement en quelques secondes pour fournir une alimentation électrique d'urgence suffisante pour alimenter le centre de données à pleine capacité généralement pendant plusieurs jours.

Systèmes d'exploitation des serveurs. Les serveurs Google utilisent des systèmes d'exploitation renforcés et personnalisés en fonction des besoins uniques en termes de serveurs de l'entreprise. Les données sont stockées à l'aide d'algorithmes propriétaires afin de renforcer la redondance et la sécurité des données. Google examine le code de manière à renforcer la sécurité de celui utilisé pour assurer les Services de sous-traitance et à améliorer les produits de sécurité dans les environnements de production.

Continuité des activités. Google réplique les données sur plusieurs systèmes pour mieux les protéger contre les destructions ou les pertes accidentelles. Google a conçu des plans de continuité d'activité et des programmes de reprise après sinistre, et les planifie et les teste régulièrement.

(b) **Réseaux et transmission.**

Transmission de données. Les centres de données sont généralement connectés à l'aide de lignes privées à vitesse élevée pour assurer des transferts de données sûrs et rapides entre les centres de données. Par ailleurs, Google chiffre les données transmises entre les centres de données. Cette opération vise à empêcher la lecture, la copie, la modification et la suppression non autorisée des données au cours du transport électronique de celles-ci. Google transfère les données selon les protocoles Internet standards.

Surface d'attaque externe. Google utilise plusieurs couches d'appareils réseau et de détection des intrusions afin de protéger sa surface d'attaque externe. Google tient compte des vecteurs d'attaque potentiels et intègre des technologies dédiées à ses systèmes externes.

Détection des intrusions. La détection des intrusions sert à fournir des informations sur les activités en cours liées à des attaques et sur la manière de réagir face aux incidents. La détection des intrusions de Google repose sur les procédures suivantes:

1. Surveillance étroite de la taille et de la composition de la surface d'attaque de Google par le biais de mesures préventives
2. Mise en place de contrôles de détection intelligents aux points d'entrée des données
3. Utilisation de technologies permettant de remédier automatiquement à certaines situations dangereuses

Gestion des incidents. Google surveille divers canaux de communication en lien avec les incidents de sécurité. De plus, le personnel de sécurité de Google réagit rapidement aux incidents connus.

Technologies de chiffrement Google exploite le chiffrement HTTPS (également appelé connexion TLS). Les serveurs Google sont compatibles avec l'échange de clés cryptographiques éphémères Diffie-Hellman basé sur les courbes elliptiques. La signature est effectuée à l'aide des protocoles RSA et ECDSA. Ces méthodes de confidentialité persistante parfaite (PFS) permettent de protéger le trafic et de minimiser l'impact d'une clé compromise ou d'une percée cryptographique.

2. Contrôle sur site et contrôle d'accès

(a) **Contrôles sur site.**

Fonctionnement de la sécurité sur site des centre de données. La sécurité des centres de données de Google est assurée sur site. Elle vise à garantir le fonctionnement de toutes les fonctions de sécurité des centres de données physiques 24h/24, 7j/7. Les membres du personnel responsable des opérations de sécurité sur site contrôlent des caméras en circuit fermé ("caméras de surveillances") et tous les systèmes d'alarme. Les membres du personnel en charge des opérations de sécurité sur site effectuent régulièrement des rondes à l'intérieur et à l'extérieur du centre de données.

Procédures d'accès aux centres de données. Google applique des procédures d'accès formelles pour autoriser un accès physique aux centres de données. Les centres de données sont installés dans des complexes dont l'accès se fait à l'aide d'une clé électronique et qui disposent d'alarmes reliées au centre de sécurité sur site. Toutes les personnes qui accèdent au centre de données sont tenues de s'identifier et de présenter une preuve d'identité au personnel de sécurité. Seuls les employés, les prestataires et les visiteurs autorisés peuvent entrer dans les centres de données. Seuls les employés et les prestataires autorisés peuvent demander une clé électronique en vue d'accéder à ces complexes. Les demandes de clés électroniques d'accès doivent être formulées à l'avance et par écrit. Elles doivent être approuvées par le personnel autorisé du centre de données. Toute autre personne accédant temporairement au centre de données doit: (i) obtenir l'autorisation préalable du personnel autorisé du centre de données pour l'accès au centre de données concerné et aux espaces intérieurs qu'elle souhaite visiter; (ii) s'inscrire auprès de l'équipe de sécurité sur site; et (iii) présenter une autorisation prouvant qu'elle est autorisée à accéder au centre de données.

Appareils de sécurité sur site des centres de données. Les centres de données de Google ont recours à un système de contrôle des accès biométrique fonctionnant à l'aide de cartes électroniques. Celui-ci est relié à un système d'alarme. Le système de contrôle des accès surveille et enregistre la carte électronique de chaque individu, ainsi que les franchissements des portes du périmètre et des zones d'expédition et de réception, ainsi que d'autres zones critiques. Les activités non autorisées et les tentatives d'accès ayant échoué sont enregistrées par le système de contrôle des accès et font l'objet d'un examen approprié. L'accès autorisé aux activités et aux centres de données dépend des zones et des responsabilités liées aux tâches de l'individu. Les portes coupe-feu du centre de données sont équipées d'alarmes. Des caméras de surveillance sont présentes tant à l'intérieur qu'à l'extérieur des centres de données. La position des caméras a été pensée de manière à couvrir des zones stratégiques telles que le périmètre, les portes du bâtiment du centre de données, et les zones de livraison et de réception, entre autres. Le personnel chargé de la gestion de la sécurité sur site est responsable des équipements de contrôle, d'enregistrement et de surveillance par caméras. Dans les centres de données, les équipements de surveillance sont reliés à l'aide de câbles. Les caméras enregistrent les images du site grâce à des enregistreurs vidéo numériques 24h/24, 7j/7. Les enregistrements de surveillance sont conservés pendant au moins sept jours, en fonction de l'activité.

(b) **Contrôle des accès.**

Personnel de sécurité des infrastructures. Google a mis en place et applique des règles de sécurité pour son personnel, qui doit obligatoirement suivre une formation à la sécurité dans le cadre de sa formation globale. Le personnel de sécurité des infrastructures de Google est responsable du contrôle continu des infrastructures de sécurité de Google, de l'examen des Services de sous-traitance et de la réponse aux incidents de sécurité.

Contrôle des accès et gestion des droits. Les administrateurs et utilisateurs du client doivent s'authentifier par l'intermédiaire d'un système d'authentification central ou d'authentification

unique afin d'utiliser les Services de sous-traitance.

Processus et règles d'accès aux données internes – Règlement d'accès. Les processus et règles de Google concernant l'accès aux données internes visent à empêcher les personnes et/ou les systèmes non autorisés d'accéder aux systèmes de traitement des données personnelles. Avec ses systèmes, Google vise à: (i) permettre, uniquement aux personnes habilitées, d'accéder aux données pour lesquelles elles disposent d'une autorisation; et (ii) s'assurer que les données personnelles ne peuvent pas être consultées, copiées, modifiées ou supprimées sans autorisation pendant le traitement et l'utilisation ainsi qu'après l'enregistrement. Les systèmes permettent de détecter les accès inappropriés. Google a recours à un système de gestion des accès centralisé pour contrôler les accès des membres du personnel aux serveurs de production. Google permet par ailleurs à un nombre limité des membres du personnel d'y accéder. LDAP, Kerberos et un système propriétaire utilisant des certificats numériques sont conçus pour fournir à Google des mécanismes d'accès sûrs et flexibles. Ces mécanismes n'octroient que les droits d'accès approuvés aux hôtes des sites, aux journaux, aux données et aux informations de configuration. Google requiert l'utilisation d'ID utilisateur uniques, de mots de passe sécurisés, de l'authentification à deux facteurs et de listes d'accès surveillées attentivement pour réduire le risque potentiel d'utilisation non autorisée des comptes. L'octroi ou la modification des accès sont basés sur les éléments suivants: les responsabilités liées aux tâches du personnel autorisé, les exigences liées aux tâches autorisées et le besoin de connaître. De plus, l'octroi et la modification des droits d'accès doivent être réalisés conformément aux règles et aux formations internes de Google en matière d'accès aux données. Les approbations sont gérées par les outils de workflow qui conservent les enregistrements d'audit de toutes les modifications. Tout accès aux systèmes est enregistré dans un journal d'audit. Lorsque des mots de passe sont employés pour l'authentification (pour la connexion aux postes de travail, par exemple), les règles concernant les mots de passe qui sont au moins conformes aux pratiques standards de l'industrie sont appliquées. Ces pratiques standards incluent entre autres les restrictions liées à la réutilisation des mots de passe et à leur niveau de sécurité minimal.

3. Données

(a) **Authentification, isolement et stockage des données.**

Google stocke les données dans un environnement mutualisé, sur des serveurs qui lui appartiennent. Les données, la base de données des Services de sous-traitance et l'architecture des systèmes de fichiers sont dupliqués et répartis entre plusieurs centres de données situés à des endroits différents. Google isole les données de chaque client de façon logique. Un système d'authentification central est utilisé pour tous les Services de sous-traitance afin d'augmenter la sécurité uniforme des données.

(b) **Consignes liées à la mise hors service et à la destruction des disques.**

Certains disques contenant des données peuvent rencontrer des problèmes de performances, des erreurs ou des pannes matérielles engendrant leur mise hors service (“**Disque hors service**”). Chaque Disque hors service est soumis à des processus de destruction des données (les “**Consignes de destruction des données**”) avant de quitter les locaux de Google en vue de leur réutilisation ou de leur destruction. Les Disques hors service sont effacés selon un processus en plusieurs étapes et validés par au moins deux experts indépendants. Les résultats du processus d'effacement sont consignés avec le numéro de série du Disque hors service à des fins de suivi. Enfin, le Disque hors service effacé est replacé dans l'inventaire afin de pouvoir être réutilisé et

redéployé. Si, en raison d'une défaillance matérielle, le Disque hors service ne peut pas être effacé, il est stocké de façon sécurisée jusqu'à ce que sa destruction soit possible. Chaque complexe fait régulièrement l'objet d'audits pour contrôler le respect des Consignes de destruction des données.

4. Personnel et sécurité des données

Le personnel de Google est tenu de se comporter de manière conforme aux directives de l'entreprise concernant la confidentialité, l'éthique commerciale, l'utilisation adéquate et les normes professionnelles. Google vérifie les antécédents dans la mesure autorisée par la loi et conformément à la loi du travail locale et aux réglementations statutaires applicables.

Le personnel doit respecter un accord de confidentialité ainsi que les règles de Google concernant la confidentialité et le respect de la vie privée, dont il doit par ailleurs accuser réception. Il reçoit aussi une formation à la sécurité. Les membres du personnel qui gèrent les données personnelles des clients doivent respecter des exigences supplémentaires associées à leur rôle. Le personnel de Google ne traite en aucun cas les données personnelles des clients sans autorisation.

5. Sous-traitants indirects et sécurité des données

Avant d'engager des Sous-traitants indirects, Google réalise un audit de leurs pratiques en matière de sécurité et de confidentialité, afin de s'assurer qu'ils garantissent un niveau de sécurité et de confidentialité approprié, compte tenu de leur accès aux données et du champ d'application des services pour lesquels ils ont été recrutés. Une fois que Google a évalué les risques présentés par le Sous-traitant ultérieur, celui-ci doit accepter des conditions contractuelles appropriées en termes de sécurité, de confidentialité et de vie privée, conformément aux exigences stipulées dans la Section 11.3 (Exigences relatives au recours à des Sous-traitants ultérieurs).

Annexe 3 : Conditions Supplémentaires pour la Législation Non-Européenne en matière de protection des données

Les Conditions Supplémentaires pour la Législation Non-Européenne en matière de protection des données suivantes complètent les présentes Conditions de traitement des données :

- CCPA Addendum applicable aux Prestataires de Service disponible sur privacy.google.com/businesses/processorterms/ccpa (daté du 1er janvier 2020)

Conditions de traitement des données Google Ads, Version 2.0

12 Août 2020

Versions précédentes

- 1 janvier 2020
- 31 octobre 2019
- 12 octobre 2017