Conditions Google Ads relatives au traitement des données

Google et la partie co-contractante qui accepte les présentes conditions (le "**Client**") ont conclu un accord pour la fourniture des Services de sous-traitance (l'"**Accord**", tel que modifié périodiquement).

Les présentes Conditions Google Ads relatives au traitement des données (y compris les annexes, les "**Conditions relatives au traitement des données**") sont conclues par Google et le Client, et complètent l'Accord. Les présentes Conditions relatives au traitement des données entreront en vigueur et remplaceront toutes les conditions précédemment applicables 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 relatives au traitement des données pour le compte du Client, vous garantissez que : (a) vous jouissez de la capacité juridique nécessaire pour engager le Client au respect des présentes Conditions relatives au traitement des données ; (b) vous avez lu et compris les présentes Conditions relatives au traitement des données ; et (c) vous acceptez, pour le compte du Client, les présentes Conditions relatives au traitement des données. Si vous n'avez pas la capacité juridique d'engager le Client, veuillez ne pas accepter les présentes Conditions relatives au traitement des données.

1. Introduction

Les présentes Conditions relatives au 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

2.1 Dans le cadre des présentes Conditions relatives au traitement des données :

"**Produit supplémentaire**" désigne une application, un produit ou un service fournis par Google ou un tiers qui : (a) ne font pas partie des Services de sous-traitance ; et (b) sont accessibles pour une utilisation dans l'interface utilisateur des Services de sous-traitance, ou sont autrement intégrés aux Services de sous-traitance.

"**Conditions supplémentaires liées à la législation non européenne en matière de protection des données**" désigne les conditions supplémentaires mentionnées en Annexe 3, qui reflètent l'accord des parties sur le traitement de certaines données dans le cadre de certaines Législations non européennes en matière de protection des données.

"**Pays approprié**" désigne :

(a) pour les données traitées soumises au RGPD de l'UE : l'EEE, ou un pays ou un territoire concerné par une décision d'adéquation de la Commission conformément à l'Article 45(1) du RGPD de l'UE ;

(b) pour les données traitées soumises au RGPD du Royaume-Uni : le Royaume-Uni, ou un pays ou un territoire concerné par des réglementations d'adéquation conformément à l'Article 45(1) du RGPD du Royaume-Uni et à la Section 17A du Data Protection Act 2018 ; et/ou

(c) pour les données traitées soumises à la Loi fédérale suisse sur la protection des données (LPD) : la Suisse, ou un pays ou un territoire (i) figurant sur la liste des États dont la législation assure un niveau adéquat de protection tel que publié par le Préposé fédéral suisse à la protection des données et à la transparence (PFPDT), ou (ii) concerné par une décision d'adéquation du Conseil fédéral suisse conformément à la LPD suisse.

"**Solution de transfert alternative**" désigne une solution, autre que les Clauses contractuelles types, qui permet le transfert légal de données à caractère personnel vers un pays tiers, conformément à la Législation européenne en matière de protection des données.

"**Données à caractère personnel du client**" désigne les données à caractère personnel traitées par Google au nom du Client dans le cadre de la fourniture par Google des Services de sous-traitance.

"**Clauses contractuelles types du client**" désigne les Clauses contractuelles types (Responsable du traitement-Sous-traitant dans l'UE), les Clauses contractuelles types (Sous-traitant-Responsable du traitement dans l'UE), les Clauses contractuelles types (Sous-traitant-Sous-traitant dans l'UE) et/ou les Clauses contractuelles types (Responsable du traitement-Sous-traitant au Royaume-Uni), selon le cas.

"**Incident lié aux données**" désigne une violation de la sécurité de Google entraînant la destruction, perte, modification, divulgation non autorisée, ou un accès accidentel ou illicite aux Données à caractère personnel du client sur des systèmes gérés ou contrôlés par Google Les "Incidents liés aux données" n'incluent pas les tentatives ni les activités infructueuses ne compromettant pas la sécurité des Données à caractère personnel 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 la disposition des personnes concernées par une Entité Google, et permettant à Google de répondre directement et de manière standardisée à certaines demandes des personnes concernées à propos des Données à caractère personnel du client (par exemple, les paramètres de publicité en ligne ou le plugin du navigateur).

"**EEE**" désigne l'Espace économique européen.

"**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.

"**Législation européenne en matière de protection des données**" désigne, selon le cas : (a) le RGPD ; et/ou (b) la LPD suisse.

"**Législation européenne**" désigne, 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 des Données à caractère personnel du client) ; et (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 à caractère personnel du client).

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

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

"**Entité Google**" désigne Google LLC (anciennement Google Inc.), Google Ireland Limited ou toute autre entité qui, directement ou indirectement, contrôle, est contrôlée par, ou est sous le contrôle commun de, Google LLC.

"**Consignes**" a la signification donnée à la Section 5.2 (Consignes du Client).

"**Certification ISO 27001**" désigne la Certification ISO/IEC 27001:2013 ou une certification comparable pour les Services de sous-traitance.

"**Nouveau sous-traitant indirect**" a la signification donnée à la Section 11.1 (Consentement à l'engagement de sous-traitants indirects).

"**Législation non européenne en matière de protection des données**" désigne les lois relatives à la protection des données ou à la vie privée en vigueur en dehors de l'EEE, du Royaume-Uni et de la Suisse.

"**Adresse e-mail de notification**" désigne l'adresse e-mail 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 relatives au traitement des données.

"**Services de sous-traitance**" désigne les services applicables listés à l'adresse business.safety.google/adsservices.

"**Clauses contractuelles types**" désigne les Clauses contractuelles types du client et/ou les Clauses contractuelles types (Responsable du traitement-Responsable du traitement dans l'UE, Google Exporter), selon le cas.

"**Clauses contractuelles types (Responsable du traitement-Sous-traitant dans l'UE)**" désigne les conditions disponibles à l'adresse business.safety.google/adsprocessorterms/sccs/eu-c2p.

"**Clauses contractuelles types (Sous-traitant-Responsable du traitement dans l'UE)**" désigne les conditions disponibles à l'adresse business.safety.google/adsprocessorterms/sccs/eu-p2c.

"**Clauses contractuelles types (Sous-traitant-Sous-traitant dans l'UE)**" désigne les conditions disponibles à l'adresse business.safety.google/adsprocessorterms/sccs/eu-p2p.

"**Clauses contractuelles types (Sous-traitant-Sous-traitant dans l'UE, Google Exporter)**" désigne les conditions disponibles à l'adresse business.safety.google/adsprocessorterms/sccs/eu-p2p-intra-group.

"**Clauses contractuelles types (Responsable du traitement-Sous-traitant au Royaume-Uni)**" désigne les conditions disponibles à l'adresse business.safety.google/adsprocessorterms/sccs/uk-c2p.

"**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 dans la Section 7.1.1 (Mesures de sécurité de Google).

“**Sous-traitants indirects**” désigne les tiers autorisés en vertu des présentes conditions relatives au traitement des données à avoir un accès logique aux Données à caractère personnel du client et à les traiter afin de fournir une partie des Services de sous-traitance et tout support technique associé.

“**Autorité de contrôle**” désigne, selon le cas : (a) une "autorité de contrôle" telle que définie dans le RGPD de l'UE ; et/ou (b) le "Commissioner" (Préposé) tel que défini dans le RGPD du Royaume-Uni et/ou la LPD suisse.

“**LPD suisse**” désigne la loi fédérale suisse sur la protection des données du 19 juin 1992.

“**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.

“**Date d'entrée en vigueur des conditions**” désigne, selon le cas :

(a) le 25 mai 2018, si le Client ou les parties ont accepté les présentes Conditions relatives au traitement des données à cette date ou à une date antérieure ; ou

(b) la date à laquelle le Client ou les parties ont accepté les présentes Conditions relatives au traitement des données, s'ils l'ont fait après le 25 mai 2018.

“**RGPD du Royaume-Uni**” désigne le RGPD de l'UE tel qu'amendé et incorporé dans la législation du Royaume-Uni, en application du European Union (Withdrawal) Act 2018, et la législation secondaire applicable émise dans le cadre du European Union (Withdrawal) Act 2018.

2.2 Les termes “**responsable du traitement**”, “**personne concernée**”, “**données à caractère personnel**”, “**traitement**” et “**sous-traitant**” tels qu'utilisés dans les présentes Conditions relatives au traitement des données ont la signification donnée dans le RGPD. Les termes “**importateur de données**” et “**exportateur de données**” ont la signification donnée dans les Clauses contractuelles types applicables.

2.3 Les termes “**incluant**” et “**y compris**” signifient "y compris, mais sans s'y limiter". Les exemples utilisés dans les présentes Conditions relatives au traitement des données ne sont fournis qu'à titre illustratif et ne constituent pas les seuls exemples d'un concept donné.

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

2.5 Dans le cas où la version traduite des présentes Conditions relatives au traitement des données n'est pas cohérente avec la version en anglais, la version en anglais prévaut.

3. Durée des présentes Conditions relatives au traitement des données

Les présentes Conditions relatives au traitement des données prendront effet à la Date d'entrée en vigueur des Conditions. Que l'Accord ait été résilié ou qu'il ait expiré, les présentes Conditions relatives au traitement des données resteront en vigueur jusqu'à ce que Google supprime toutes les Données à caractère personnel du client et qu'elles expirent automatiquement, tel que décrit dans les présentes Conditions relatives au traitement des données.

4. Application des présentes Conditions relatives au 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) (incluses) ne s'appliqueront que dans la mesure où la Législation européenne en matière de protection des données s'applique au traitement des Données à caractère personnel du client, y compris si :

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

(b) les Données à caractère personnel du client sont des données à caractère personnel 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 dans l'EEE ou au Royaume-Uni.

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

4.3 **Intégration des Conditions supplémentaires liées à la législation non européenne en matière de protection des données**. Les Conditions supplémentaires liées à la législation non européenne en matière de protection des données s'ajoutent aux présentes Conditions relatives au traitement des données.

5. Traitement des données

5.1 **Rôles, conformité réglementaire et 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 à caractère personnel du client ;

(b) Google est sous-traitant des Données à caractère personnel du client conformément à la Législation européenne en matière de protection des données ;

(c) le Client est responsable du traitement ou sous-traitant, selon le cas, des Données à

caractère personnel 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 à caractère personnel du client.

5.1.2 **Clients sous-traitants**. Si le Client est un sous-traitant :

(a) Le Client garantit en continu que le responsable du traitement concerné a autorisé : (i) les Consignes, (ii) la nomination par le Client de Google en tant qu'autre sous-traitant et (iii) l'engagement par Google de sous-traitants indirects, tel que décrit dans la Section 11 (Sous-traitants indirects) ;

(b) Le Client transfèrera immédiatement au responsable du traitement concerné toute notification de Google en vertu des Sections 5.4 (Notifications de Consignes), 7.2.1 (Notification d'Incident), 11.4 (Possibilité d'opposition aux changements de Sous-traitants indirects) ou en lien avec des Clauses contractuelles types ; et

(c) Le Client peut mettre à la disposition du responsable du traitement concerné toute information rendue disponible par Google en vertu des Sections 7.4 (Certification de sécurité), 10.6 (Informations concernant les centres de données) et 11.2 (Informations concernant les Sous-traitants indirects).

5.2 **Consignes du Client**. En acceptant les présentes Conditions relatives au traitement des données, le Client demande à Google de traiter les Données à caractère personnel 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 relatives au 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 relatives au traitement des données (collectivement, les **Consignes**).

5.3 **Respect des Consignes par Google**. Google se conformera aux Consignes, sauf si la Législation européenne l'interdit.

5.4 **Notifications de Consignes**. Google notifiera immédiatement le Client si, d'après Google : (a) la Législation européenne ne permet pas à Google de respecter une Consigne ; (b) une Consigne ne respecte pas la Législation européenne en matière de protection des données ; ou (c) Google n'est pas en mesure de respecter une Consigne, à moins qu'une telle notification soit interdite par la Législation européenne. La présente Section 5.4 (Notifications de Consignes) ne limite les droits et obligations d'aucune des parties prévus par le reste de l'Accord.

5.5 **Produits supplémentaires**. Si le Client utilise des Produits supplémentaires, les Services de sous-traitance peuvent permettre à ces Produits supplémentaires d'accéder aux Données à caractère personnel du client, comme le requiert l'interopérabilité de ces Produits supplémentaires avec les Services de sous-traitance. Pour plus de clarté, les présentes Conditions relatives au traitement des données ne s'appliquent pas au traitement des données à caractère personnel en relation avec la fourniture des Produits supplémentaires utilisés par le Client, y compris les données à caractère

personnel transmises vers ou à partir de ces Produits supplémentaires.

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 à caractère personnel du client ;

(b) le Client utilise les Services de sous-traitance pour supprimer certaines Données à caractère personnel du client ; et

(c) les Données à caractère personnel du client supprimées ne peuvent pas être récupérées par le Client (par exemple, à partir de la "corbeille"),

alors Google supprimera lesdites Données à caractère personnel du client de ses systèmes dès que possible et dans un délai maximal de 180 jours, sauf si la Législation européenne ou nationale en 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 à caractère personnel 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). Avant une telle suppression, Google fournira au Client des informations supplémentaires sur les frais applicables et la façon dont ils sont calculés.

6.2 **Suppression à l'expiration de la Durée**. Le Client demande à Google de supprimer toutes les données à caractère personnel du Client restantes (y compris les copies existantes) des systèmes de Google à la fin de la Durée, conformément à la législation en vigueur. Google se conformera à cette consigne dès que possible et dans un délai maximal de 180 jours, sauf si la Législation européenne exige le stockage.

7. Sécurité des données

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

7.1.1 **Mesures de sécurité de Google**. Google mettra en œuvre et maintiendra des mesures techniques et organisationnelles adéquates pour protéger les Données à caractère

personnel du client contre une destruction, une perte, une altération, une divulgation ou un accès non autorisés, accidentels ou illicites, tel que décrit en Annexe 2 (**Mesures de sécurité**). Comme décrit en Annexe 2, les Mesures de sécurité comprennent des mesures pour : (a) chiffrer les données à caractère personnel ; (b) contribuer à garantir la confidentialité, l'intégrité, la disponibilité, et la résilience des systèmes et services de Google ; (c) aider à rétablir rapidement l'accès aux données à caractère personnel à la suite d'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 **Accès et conformité**. Google : (a) autorisera ses employés, ses prestataires et ses sous-traitants indirects à accéder aux Données à caractère personnel du client uniquement si cela s'avère strictement nécessaire pour respecter les Consignes ; (b) prendra les mesures appropriées pour s'assurer que ses employés, ses prestataires et ses sous-traitants indirects respectent les Mesures de sécurité dans la mesure applicable à l'étendue de leur prestation ; et (c) veillera à ce que toutes les personnes autorisées à traiter les Données à caractère personnel 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**. Google (en tenant compte de la nature du traitement des Données à caractère personnel du client et des informations à la disposition de Google) aidera le Client à assurer le respect des obligations du Client (ou, si le Client est un sous-traitant, les obligations du responsable du traitement concerné) en ce qui concerne la sécurité des données à caractère personnel et les violations des données à caractère personnel, y compris les obligations du Client (ou, si le Client est un sous-traitant, les obligations du responsable du traitement concerné) en vertu des Articles 32 à 34 (inclus) du RGPD :

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

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

(c) en 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 relatives au 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 concerné par l'Incident de données rapidement et sans retard injustifié ; et (b) prendra rapidement des mesures raisonnables pour minimiser les dommages et sécuriser les Données à caractère personnel du client.

7.2.2 **Détails de l'Incident de données**. Les notifications créées conformément à la Section 7.2.1 (Notification d'Incident) décriront : la nature de l'Incident de données, y compris les ressources du Client concernées ; les mesures prises par Google ou que Google a l'intention de prendre pour régler l'Incident de données et en atténuer les risques potentiels ; les mesures, le cas échéant, que Google recommande au Client de prendre pour régler

l'Incident de données ; et les coordonnées d'un contact qui pourrait fournir plus d'informations. S'il n'est pas possible de fournir toutes ces informations en même temps, la notification initiale de Google contiendra les informations disponibles à ce moment-là. Les autres seront fournies sans retard injustifié à mesure qu'elles sont disponibles.

7.2.3 **Communication des notifications**. Google communiquera 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 d'Adresse e-mail de notification), par un autre moyen de communication direct (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 tierces**. 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 d'un Incident de données, ou sa réponse à un tel Incident, 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 du Client en matière de sécurité et évaluation de celle-ci**.

7.3.1 **Responsabilités du Client en matière de sécurité**. 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 adapté au risque en ce qui concerne les Données à caractère personnel 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 à caractère personnel du client que le Client choisit de stocker ou de transférer hors des systèmes de Google et de ses sous-traitants indirects.

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

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 auditeur tiers désigné par le Client à effectuer des audits (y compris des inspections) afin de vérifier que Google respecte ses obligations en vertu des présentes Conditions relatives au traitement des données conformément à la Section 7.5.3 (Conditions commerciales supplémentaires pour les audits). Pendant un audit, Google rendra disponibles toutes les informations nécessaires pour démontrer cette conformité et contribuer aux audits, tel que décrit dans la Section 7.4 (Certification de sécurité) et dans la présente Section 7.5 (Examens et audits de conformité).

(b) Si les Clauses contractuelles types s'appliquent en vertu de la Section 10.3 (Transferts limités), Google autorisera le Client (ou un auditeur tiers nommé par le Client) à réaliser des audits, tel que décrit dans les Clauses contractuelles types. Pendant l'audit, Google rendra disponibles toutes les informations requises en vertu des 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 relatives au traitement des données en examinant le certificat délivré pour la Certification ISO 27001 (qui reflète le résultat d'un audit mené par un auditeur 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 s'accorderont à l'avance sur la date de début raisonnable, la portée et la durée de tout audit, ainsi que sur les paramètres de sécurité et de confidentialité applicables, conformément à la Section 7.5.2(a) ou 7.5.2(b).

(c) Google peut facturer des frais (sur la base des coûts raisonnables de Google) pour tout audit en vertu de la Section 7.5.2(a) ou 7.5.2(b). Avant tout audit, Google fournira au Client des informations supplémentaires sur les frais applicables et la façon dont ils sont calculés. Le Client sera responsable de tous les frais facturés par tout auditeur tiers nommé par le Client pour exécuter un tel audit.

(d) Google peut s'opposer à tout auditeur tiers nommé par le Client pour effectuer un audit en vertu de la Section 7.5.2(a) ou 7.5.2(b) si l'auditeur, 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

auditeur ou à mener l'audit lui-même.

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

8. Analyses d'impact et consultations

Google (en tenant compte de la nature du traitement et des informations à la disposition de Google) aidera le Client à assurer le respect des obligations du Client (ou, si le Client est un sous-traitant, les obligations du responsable du traitement concerné) 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 ou du responsable du traitement concerné conformément aux Articles 35 et 36 du RGPD :

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

(b) en fournissant les informations contenues dans l'Accord (y compris les présentes Conditions relatives au traitement des données) ; et

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

9. Droits des personnes concernées

9.1 **Réponses aux demandes des personnes concernées**. Si Google reçoit une demande d'une personne concernée au sujet des Données à caractère personnel du client, le Client autorise Google à, et Google avertit par les présentes le Client qu'il va :

(a) répondre directement à la demande de la personne concernée conformément à la

fonctionnalité standard de l'outil mis à la disposition des personnes concernées (si la demande est envoyée à l'aide d'un tel outil) ; ou

(b) conseiller à la personne concernée d'envoyer sa demande au Client. Le Client sera alors tenu d'y répondre (si la demande n'est pas envoyée à l'aide d'un outil mis à la disposition des personnes concernées).

9.2 **Assistance apportée par Google pour les demandes des personnes concernées**. Conformément au Chapitre III du RGPD, Google aidera le Client à remplir ses obligations (ou, si le Client est un sous-traitant, les obligations du responsable du traitement concerné) de répondre aux demandes d'exercice des droits des personnes concernées, dans tous les cas en tenant compte de la nature du traitement des Données à caractère personnel du client et, le cas échéant, de l'Article 11 du RGPD :

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

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

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

9.3 **Rectification**. Si le Client constate que des Données à caractère personnel du client sont imprécises ou obsolètes, et si la Législation européenne en matière de protection des données l'exige, le Client sera tenu de les rectifier ou de les supprimer, y compris (si disponible) à l'aide de la fonctionnalité des Services de sous-traitance.

10. Transferts de données

10.1 **Stockage des données et sites de traitement**. Sous réserve de la présente Section 10 (Transferts de données), Google peut traiter les Données à caractère personnel du client dans tous les pays dans lesquels Google ou l'un de ses Sous-traitants indirects dispose de sites.

10.2 **Transferts autorisés**. Les parties reconnaissent que la Législation européenne en matière de protection des données ne requiert pas de Clauses contractuelles types ni de Solution de transfert alternative pour traiter les Données à caractère personnel du client ou pour les transférer dans un Pays approprié (**Transferts autorisés**).

10.3 **Transferts limités**. Si le traitement des Données à caractère personnel du client implique des transferts qui ne sont pas autorisés, et que la Législation européenne en matière de protection des données s'applique à ces transferts (**Transferts limités**) :

(a) si Google annonce qu'il adopte une Solution de transfert alternative pour les Transferts limités, alors Google s'assurera qu'ils sont conformes à cette Solution de transfert alternative ; et/ou

(b) si Google n'a pas adopté de Solution de transfert alternative pour aucun Transfert limité, alors :

(i) si l'adresse de Google se trouve dans un Pays approprié :

(A) les Clauses contractuelles types (Responsable du traitement-Responsable

du traitement dans l'UE, Google Exporter) s'appliqueront pour tous les Transferts limités entre Google et des Sous-traitants indirects ; et

(B) en plus, si l'adresse du Client ne se trouve pas dans un Pays approprié, les Clauses contractuelles types (Sous-traitant-Responsable du traitement dans l'UE) s'appliqueront pour les Transferts limités entre Google et le Client (que le Client soit un responsable du traitement et/ou un sous-traitant) ; ou

(ii) si l'adresse de Google ne se trouve pas dans un Pays approprié :

(A) les Clauses contractuelles types (Responsable du traitement-Sous-traitant dans l'UE) et/ou les Clauses contractuelles types (Responsable du traitement-Responsable du traitement dans l'UE) s'appliqueront (en fonction de si le Client est un responsable du traitement et/ou un sous-traitant) pour les Transferts limités entre le Client et Google qui sont soumis au RGPD de l'UE et/ou à la LPD suisse ; et

(B) les Clauses contractuelles types (Responsable du traitement-Sous-traitant au Royaume-Uni) s'appliqueront (que le Client soit un responsable du traitement et/ou un sous-traitant) pour les Transferts limités entre le Client et Google qui sont soumis au RGPD du Royaume-Uni.

10.4 **Informations et mesures supplémentaires**. Google fournira au Client des informations concernant les Transferts limités, y compris des informations sur des mesures supplémentaires visant à protéger les Données à caractère personnel du client, tel que décrit dans la Section 7.5.1 (Examens de la Documentation de sécurité), dans l'Annexe 2 (Mesures de sécurité) et dans d'autres documents au sujet de la nature des Services de sous-traitance et du traitement des Données à caractère personnel du client (par exemple, les articles du centre d'aide).

10.5 **Résiliation**. Si le Client constate que, sur la base de son utilisation actuelle ou de l'utilisation qu'il prévoit de faire des Services de sous-traitance, la Solution de transfert alternative et/ou les Clauses contractuelles types, selon le cas, n'offrent pas de protection appropriée pour les Données à caractère personnel du client, alors le Client peut immédiatement mettre un terme à l'Accord par souci de commodité en informant Google par écrit.

10.6 **Informations concernant les centres de données**. Les informations concernant les emplacements des centres de données Google sont disponibles à l'adresse www.google.com/about/datacenters/locations/.

11. Sous-traitants indirects

11.1 **Consentement à l'engagement de Sous-traitants indirects**. Le Client autorise spécifiquement l'engagement en tant que Sous-traitant indirect des entités listées à compter de la Date d'entrée en vigueur des conditions disponibles à l'URL spécifiée à la Section 11.2 (Informations concernant les Sous-traitants indirects). Par ailleurs, sans préjudice de la Section 11.4 (Possibilité d'opposition aux changements de Sous-traitant indirect) le Client autorise de façon générale l'engagement de tiers en tant que Sous-traitant indirect (**Nouveau sous-traitant indirect**).

11.2 **Informations concernant les Sous-traitants indirects**. Les informations concernant les Sous-

traitants indirects sont disponibles à l'adresse business.safety.google/adssubprocessors.

11.3 **Exigences concernant l'engagement de Sous-traitants indirects**. En ayant recours à un Sous-traitant indirect, Google :

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

(i) le Sous-traitant indirect accède aux Données à caractère personnel du client et les utilise 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 relatives au traitement des données) ; et

(ii) si le traitement des Données à caractère personnel du client est soumis à la Législation européenne en matière de protection des données, les obligations de protection des données dans les présentes Conditions relatives au traitement des données (telles qu'énoncées dans l'Article 28(3) du RGPD, le cas échéant) s'appliquent au Sous-traitant indirect ;

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

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

(a) Lorsqu'un nouveau Sous-traitant indirect est engagé pendant la Durée, Google informera le Client, au moins 30 jours avant que le nouveau Sous-traitant indirect traite des Données à caractère personnel du client, de l'engagement (y compris le nom et la localisation du sous-traitant indirect 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 indirect en résiliant l'Accord immédiatement par 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 indirect tel que décrit à la Section 11.4(a).

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 relatives au traitement des données via les méthodes décrites sur privacy.google.com/businesses/processorsupport ou via d'autres moyens fournis par Google ponctuellement. Google fournira une assistance rapide et raisonnable en réponse aux demandes du Client que Google reçoit via de tels moyens et qui sont liées au traitement des Données à caractère personnel du client dans le cadre de l'Accord.

12.2 **Registre des traitements de Google**. Google conservera les documents appropriés de ses activités de traitement, tel que requis par le RGPD. Le Client reconnaît que Google est tenu par le RGPD de : (a) recueillir et conserver 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.

12.3 **Demandes du responsable du traitement**. Si Google reçoit une demande ou une instruction via les méthodes décrites dans la Section 12.1 (ou via d'autres méthodes) de la part d'une tierce partie prétendant être un responsable du traitement des Données à caractère personnel du client, Google conseillera à la tierce partie de contacter le Client.

13. Responsabilité

Si l'Accord est gouverné 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 des présentes Conditions relatives au traitement des données ou en relation avec celles-ci sera limitée à la valeur monétaire ou au paiement maximal auquel la responsabilité de cette partie est plafonnée en vertu de l'Accord (aucune exclusion de demande d'indemnisation issue des clauses limitatives de responsabilité de l'Accord ne sera donc 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 des présentes Conditions relatives au traitement des données ou en relation avec celles-ci sera soumise aux exclusions et aux limitations de responsabilité figurant dans l'Accord.

14. Conséquences des présentes Conditions relatives au traitement des données

14.1 **Ordre de priorité**. En cas de conflit ou d'incohérence entre les Clauses contractuelles types du client, les Conditions supplémentaires liées à la législation non européenne en matière de protection des données, le reste des présentes Conditions relatives au traitement des données et/ou le reste de l'Accord, l'ordre de priorité suivant sera d'application :

(a) Clauses contractuelles types du client (si applicables) ;

(b) Conditions supplémentaires liées à la législation non européenne en matière de protection des données (si applicables)

(c) Reste des présentes Conditions relatives au traitement des données ; et

(d) Reste de l'Accord

Sous réserve des amendements contenus dans les présentes Conditions relatives au traitement des données, l'Accord reste pleinement en vigueur.

14.2 **Aucune modification des Clauses contractuelles types.** Rien dans l'Accord (y compris les présentes Conditions relatives au traitement des données) ne vise à modifier ou contredire les

Clauses contractuelles types ni à nuire aux droits fondamentaux ou aux libertés des personnes concernées en vertu de la Législation européenne en matière de protection des données.

14.3 **Aucune conséquence sur les Conditions du responsable du traitement**. Les présentes Conditions relatives au traitement des données n'auront aucune conséquence sur d'autres conditions distinctes liant Google et le Client dans une relation de type responsable du traitement-responsable du traitement pour un autre service que les Services de sous-traitance.

14.4 **Anciennes Clauses contractuelles modèles**. Le Client accepte qu'à compter de leur date d'entrée en vigueur, les Clauses contractuelles types remplacent et annulent les Clauses contractuelles modèles approuvées en vertu de l'Article 26(2) de la Directive 95/46/CE et précédemment conclues entre le Client et Google LLC (les "Clauses contractuelles modèles"). Dans les cas où Google LLC n'est pas partie à l'Accord, Google LLC sera considérée comme une tierce partie bénéficiaire de la présente Section 14.4 (Anciennes Clauses contractuelles modèles). La présente Section 14.4 (Anciennes Clauses contractuelles modèles) n'aura aucune incidence sur les droits des parties ni sur les droits des personnes concernées, qu'elles ont pu se constituer lorsque les Clauses contractuelles modèles étaient en vigueur.

15. Modifications des présentes Conditions relatives au traitement des données

15.1 **Modifications des URL**. Google peut ponctuellement modifier toute URL référencée dans les présentes Conditions relatives au traitement des données et le contenu de ces URL, mais ne peut modifier que les éléments suivants :

(a) Les Clauses contractuelles types conformément aux Sections 15.2(b) à 15.2(d) (Modifications des Conditions relatives au traitement des données) ou pour incorporer une nouvelle version des Clauses contractuelles types pouvant être adoptée en vertu de la Législation européenne en matière de protection des données, dans les deux cas d'une manière n'affectant pas la validité des Clauses contractuelles types en vertu de la Législation européenne en matière de protection des données ; et

(b) La liste de Services de sous-traitance potentiels à l'adresse business.safety.google/adsservices : (i) pour refléter tout changement du nom d'un service ; (ii) pour ajouter un service ; ou (iii) pour supprimer un service pour lequel : (x) tous les contrats de fourniture de ce service ont été résiliés ; ou (y) Google a obtenu l'autorisation du Client.

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

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

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

(c) est requise pour se conformer à la législation applicable, à la réglementation en vigueur, à une ordonnance d’un tribunal ou à une directive émise par un organisme régulateur ou une administration gouvernementale, ou si elle reflète l'adoption par Google d'une Solution de

transfert alternative ; ou

(d) (i) ne donne lieu à aucune dégradation de la sécurité globale des Services de sous-traitance ; (ii) n'étend pas la portée de, ou ne retire aucune restriction sur, (x) dans le cadre des Conditions supplémentaires liées à la législation non européenne en matière de protection des données, les droits de Google d'utiliser ou de traiter les données soumises à ces Conditions, ou (y) dans le cadre du reste des présentes Conditions relatives au traitement des données, le traitement des Données à caractère personnel du client par Google, comme décrit à la Section 5.3 (Respect des Consignes par Google) ; et (iii) n'a pas d'autre impact négatif important sur les droits du Client dans le cadre des présentes Conditions relatives au traitement des données, tel que raisonnablement déterminé par Google.

15.3 **Notification de modifications**. Si Google a l'intention de modifier les présentes Conditions relatives au 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 pouvant être requise pour se conformer à la législation applicable, à la réglementation en vigueur, à une ordonnance d'un tribunal ou à une directive émise par un organisme régulateur ou une administration gouvernementale) avant que le changement ne prenne effet : (a) en envoyant un e-mail à l'Adresse e-mail de notification ; ou (b) en 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 immédiatement par souci de commodité 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 la fin de la Durée jusqu'à la suppression de toutes les Données à caractère personnel du client par Google conformément aux présentes Conditions relatives au traitement des données.

Nature et fins du traitement

Google traitera (y compris, selon les Services de sous-traitance et les Consignes, la collecte, l'enregistrement, l'organisation, la structuration, le stockage, la modification, l'extraction, l'utilisation, la divulgation, la combinaison et l'effacement) les Données à caractère personnel du client pour fournir les Services de sous-traitance et toute assistance technique au Client conformément aux présentes Conditions relatives au traitement des données.

Types de Données à caractère personnel

Les Données à caractère personnel du client peuvent inclure les types de données à caractère personnel décrites sur business.safety.google/adsservices.

Catégories des personnes concernées

Les Données à caractère personnel du client concerneront les catégories suivantes de personnes concernées :

- les personnes concernées au sujet desquelles Google recueille des Données à caractère personnel dans le cadre de la fourniture des Services de sous-traitance ; et/ou

- les personnes concernées au sujet desquelles des Données à caractère personnel 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 d'appliquer et de garantir 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 de secours prennent le relais. Les générateurs de secours 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 opérations. 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.

Technologies de chiffrement. Les règles de sécurité de Google requièrent le chiffrement au repos de toutes les données utilisateur, y compris les données à caractère personnel. Les données sont souvent chiffrées à plusieurs niveaux dans la pile de stockage de production de Google dans les centres de données, y compris au niveau du matériel, sans action requise de la part des clients. Utiliser plusieurs couches de chiffrement renforce la protection des données et permet à Google de sélectionner l'approche optimale en fonction des exigences de l'application. Toutes les données à caractère personnel sont chiffrées au niveau du stockage, généralement à l'aide du chiffrement AES256. Google utilise des bibliothèques cryptographiques courantes qui intègrent le module validé FIPS 140-2 de Google pour implémenter le chiffrement de façon cohérente entre les Services de sous-traitance.

(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. 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 centres 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 surveillance") 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 et 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 à caractère personnel. 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 à caractère personnel 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 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.

(c) **Données pseudonymes**.

Les données sur la publicité en ligne sont généralement associées à des identifiants qui, en eux-mêmes, sont considérés comme "pseudonymes" (c'est-à-dire qu'ils ne peuvent être attribués à aucun individu spécifique sans utiliser d'informations supplémentaires). Google dispose d'un ensemble complet de règles, et de commandes techniques et organisationnelles pour assurer la séparation entre les données pseudonymes et les informations personnelles (c'est-à-dire, des informations qui pourraient permettre, en elles-mêmes, de contacter ou d'identifier directement un individu, ou de le localiser précisément) telles que les données du compte Google d'un utilisateur. Les règles Google n'autorisent les flux d'informations entre des données pseudonymes et personnelles que dans des circonstances strictement limitées.

(d) **Examens de lancement**.

Google effectue des examens de lancement pour de nouveaux produits et de nouvelles fonctionnalités avant leur lancement. Entre autres, des ingénieurs spécialement formés à la confidentialité effectuent des examens de confidentialité. Lors de tels examens, les ingénieurs spécialisés en confidentialité s'assurent que toutes les règles et consignes Google applicables sont respectées, y compris, mais sans s'y limiter, les règles en lien avec la pseudonymisation ainsi que la conservation et la suppression 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 à caractère personnel des clients doivent respecter des exigences supplémentaires associées à leur rôle. Le personnel de Google ne traite en aucun cas les données à caractère personnel 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 que présente le Sous-traitant indirect, le Sous-traitant indirect doit s'engager à respecter des conditions contractuelles appropriées en termes de sécurité, de confidentialité et de respect de la vie privée, sous réserve des exigences établies dans la Section 11.3

(Exigences concernant l'engagement de Sous-traitants indirects).

Annexe 3 : Conditions supplémentaires liées à la législation non européenne en matière de protection des données

Les Conditions supplémentaires liées à la législation non européenne en matière de protection des données suivantes s'ajoutent aux présentes Conditions relatives au traitement des données :

- Avenant au CCPA concernant les fournisseurs de services disponible à l'adresse business.safety.google/adsprocessorterms/ccpa/ (en date du 1er janvier 2020)
- Avenant à la loi LGPD destiné aux sous-traitants disponible à l'adresse business.safety.google/adsprocessorterms/lgpd/ (en date du 16 août 2020)

Conditions Google Ads relatives au traitement des données, version 3.0

27 septembre 2021

Versions précédentes

- 16 août 2020
- 12 août 2020
- 1er janvier 2020
- 31 octobre 2019
- 12 octobre 2017