Avenant relatif au traitement des données dans le cloud (Partenaires)

Le présent Avenant relatif au traitement des données dans le cloud (y compris ses annexes, l'« *Avenant* ») est intégré au Contrat (tel que défini ci-dessous) conclu entre Google et le Partenaire. Cet Avenant était auparavant appelé « Conditions relatives à la sécurité et au traitement des données » pour Google Cloud Platform et l'« Avenant relatif au traitement des données » ou « Conditions relatives à la sécurité et au traitement des données » pour les Services Looker (original) ou Google SecOps.

Conditions générales

1. Présentation

Le présent Avenant décrit les obligations des parties, y compris au titre des droits applicables relatifs à la confidentialité, la sécurité et la protection des données, pour ce qui a trait au traitement et à la sécurité des Données du Partenaire. Cet Avenant prend effet à la Date d'entrée en vigueur de l'Avenant (telle que définie ci-dessous) et remplace les éventuelles conditions précédemment applicables au traitement et à la sécurité des Données du Partenaire. Les termes commençant par une majuscule qui sont utilisés dans cet Avenant sans y être définis ont la signification qui leur est attribuée dans le Contrat.

2. Définitions

2.1 Dans le présent Avenant :

- « *Date d'entrée en vigueur de l'Avenant* » désigne la date à laquelle le Partenaire a accepté le présent Avenant ou celle à laquelle les parties sont autrement parvenues à un accord le concernant.
- « *Contrôles de sécurité supplémentaires* » désigne les ressources, fonctions, fonctionnalités et contrôles de sécurité que le Partenaire peut utiliser à sa discrétion et comme il le juge approprié, y compris la Console d'administration, le chiffrement, la journalisation et la surveillance, la gestion de l'authentification et des accès, les analyses de sécurité et les pare-feu.
- « *Contrat* » désigne le contrat en vertu duquel Google a convenu de fournir les Services concernés au Partenaire.
- « *Droit applicable relatif à la confidentialité* » désigne, pour le traitement des Données à caractère personnel du Partenaire, toute loi ou réglementation provinciale, d'un État américain,

de l'Union européenne, fédérale, nationale ou autre concernant la confidentialité, la sécurité ou la protection des données.

- « *Services audités* » désigne les Services en vigueur décrits comme entrant dans le champ d'application de la certification ou du rapport concerné disponible à l'adresse https://cloud.google.com/security/compliance/services-in-scope. Google ne peut supprimer de Services de cette URL que s'ils ont été arrêtés conformément au Contrat.

- « *Certifications de conformité* » a la signification qui lui est attribuée à la Section 7.4 (Certifications de conformité et Rapports SOC).

- « *Incident lié aux données* » désigne une violation de la sécurité de Google qui entraîne, qu'il s'agisse d'une action accidentelle ou illégale, la destruction, la perte, l'altération ou la divulgation non autorisée des Données du Partenaire stockées sur des systèmes gérés ou contrôlés par Google, ou encore l'accès non autorisé auxdites Données.

- « *EMEA* » désigne l'Europe, le Moyen-Orient et l'Afrique.

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

- « *Législation européenne sur la protection des données* » désigne, selon le cas : (a) le RGPD ou (b) la Loi fédérale sur la protection des données (LPD) de la 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 Partenaire) ; (b) la législation du Royaume-Uni ou d'une région du Royaume-Uni (si le RGPD du Royaume-Uni s'applique au traitement des Données à caractère personnel du Partenaire) ; ou (c) la législation de la Suisse (si la LPD suisse s'applique au traitement des Données à caractère personnel du Partenaire).

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

- « *Auditeur tiers de Google* » désigne un auditeur tiers indépendant et qualifié désigné par Google et dont Google divulgue au Partenaire l'identité alors connue.

- « *Instructions* » a la signification qui lui est attribuée à la Section 5.2 (Conformité avec les Instructions du Partenaire).

- « *Adresse courriel de notification* » désigne toute adresse courriel indiquée par le Partenaire dans la Console d'administration ou dans le Formulaire de commande pour recevoir certaines notifications de la part de Google.

- « *Utilisateurs finaux du Partenaire* » a la signification qui lui est attribuée dans le Contrat ou, si cette définition est manquante, a la signification qui est attribuée à « Utilisateurs finaux » dans le Contrat.

- « *Données à caractère personnel du Partenaire* » désigne les données à caractère personnel contenues dans les Données du Partenaire, y compris les catégories spéciales de données à caractère personnel ou de données sensibles définies dans le Droit applicable relatif à la confidentialité.

- « *Documentation sur la sécurité* » désigne les Certifications de conformité et les Rapports SOC.

- « *Mesures de sécurité* » a la signification qui lui est attribuée à la Section 7.1.1 (Mesures de sécurité de Google).

- « *Services* » désigne les services applicables décrits dans l'Annexe 4 (Produits spécifiques).

- « *Rapports SOC* » a la signification qui lui est attribuée à la Section 7.4 (Certifications de conformité et Rapports SOC).

- « *Sous-traitant indirect* » désigne un tiers autorisé à agir comme autre sous-traitant au titre du présent Avenant pour traiter les Données du Partenaire en vue de fournir certains Services et SAT (Services d'assistance technique).

- « *Autorité de contrôle* » désigne, selon le cas : (a) une « autorité de contrôle » telle que définie dans le RGPD de l'UE ; ou (b) le « Commissaire » tel que défini dans le RGPD du Royaume-Uni ou la LPD de la Suisse.

- « *LPD de la Suisse* » désigne, selon le cas, la Loi fédérale sur la protection des données du 19 juin 1992 (Suisse) (avec l'Ordonnance de la Loi fédérale sur la protection des données du 14 juin 1993) ou la Loi fédérale révisée sur la protection des données du 25 septembre 2020 (Suisse) (avec l'Ordonnance de la Loi fédérale sur la protection des données du 31 août 2022).

- « *Période de validité* » désigne la période commençant à la Date d'entrée en vigueur de l'Avenant et se poursuivant jusqu'à la fin de la fourniture des Services par Google, y compris, le cas échéant, toute période pendant laquelle la fourniture des Services peut être suspendue et toute période ultérieure à la résiliation pendant laquelle Google peut continuer à fournir les Services à des fins de transition.

- « *RGPD du Royaume-Uni* » désigne le RGPD de l'UE tel que modifié et incorporé dans la législation du Royaume-Uni en application de la loi de 2018 sur le retrait de l'Union européenne (European Union (Withdrawal) Act), ainsi que toutes les lois secondaires applicables conformément à ladite Loi.

2.2 Les termes « données à caractère personnel », « personne concernée », « traitement », « responsable du traitement » et « sous-traitant », tels qu'ils sont utilisés dans le présent Avenant, ont la signification qui leur est attribuée dans le Droit applicable relatif à la confidentialité ou, en l'absence de ladite définition ou dudit Droit, dans le RGPD de l'UE.

2.3 Les termes « personne concernée », « responsable du traitement » et « sous-traitant » incluent les « consommateurs », « entreprises » et « fournisseurs de service », respectivement, comme requis par le Droit applicable relatif à la confidentialité.

3. Durée

Quand bien même le Contrat serait résilié ou arrivé à expiration, le présent Avenant reste de plein effet jusqu'à ce que Google supprime toutes les Données du Partenaire comme décrit dans les présentes, et expire automatiquement au même moment.

4. Rôles ; Conformité légale

4.1 *Rôles des parties*. Google est un sous-traitant et le Partenaire est, selon le cas, un responsable du traitement ou sous-traitant des Données à caractère personnel du Partenaire.

4.2 *Résumé du traitement*. L'objet et les détails du traitement des Données à caractère personnel du Partenaire sont décrit dans l'Annexe 1 (Objet et détails du traitement des données).

4.3 *Conformité à la législation*. Chaque partie s'engage à respecter ses obligations concernant le traitement des Données à caractère personnel du Partenaire en vertu du Droit applicable relatif à la confidentialité.

4.4 *Conditions légales supplémentaires*. Lorsque le traitement des Données à caractère personnel du Partenaire est soumis à un Droit applicable relatif à la confidentialité décrit dans l'Annexe 3 (Droits spécifiques relatifs à la confidentialité), les conditions correspondantes figurant dans l'Annexe 3 s'appliquent en sus de ces Conditions générales et prévalent comme décrit à la Section 14.1 (Priorité).

5. Traitement de données

5.1 *Partenaires sous-traitants*. Si le Partenaire est un sous-traitant :

a. Le Partenaire offre une garantie continue que le Client et responsable du traitement concerné a autorisé :

i. les Instructions ;

ii. l'engagement de Google par le Partenaire en tant qu'autre sous-traitant ; et

iii. l'engagement de sous-traitants indirects par Google tel que décrit à la Section 11 (Sous-traitants indirects).

b. Le Partenaire s'engage à transmettre rapidement et sans délai indu au Client et responsable du traitement concerné tout avis fourni par Google au titre de la Section 7.2.1 (Notification des incidents), 9.2.1 (Responsabilité vis-à-vis des demandes) ou 11.4 (Possibilité de s'opposer à des Sous-traitants indirects) ; et

c. Le Partenaire peut mettre à la disposition du Client et responsable du traitement concerné toute autre information fournie par Google en vertu des présentes concernant les

emplacements des centres de données Google ou les noms, emplacements et activités des Sous-traitants indirects.

5.2 *Conformité avec les Instructions du Partenaire*. Le Partenaire demande à Google de ne traiter les Données du Partenaire conformément au Contrat (y compris au présent Avenant) que dans le but de :

a. fournir, sécuriser et surveiller les Services et SAT ; et

b. tel que spécifié :

i. lors de l'utilisation par le Partenaire des Services (y compris par le biais de la Console d'administration) et des SAT ; et

ii. dans toute autre instruction écrite fournie par le Partenaire et acceptée par Google comme instruction relevant du présent Avenant

(collectivement, les « *Instructions* »).

Google s'engage à se conformer aux Instructions à moins que la Législation européenne (lorsque la Législation européenne sur la protection des données s'applique) ou la législation applicable (lorsque tout autre Droit applicable relatif à la confidentialité s'applique) ne l'empêche.

6. Suppression des données

6.1 *Suppression par le Partenaire*. Google s'engage à permettre au Partenaire de supprimer les Données du Partenaire pendant la Période de validité, en conformité avec la fonctionnalité des Services. Si le Partenaire utilise les Services pour supprimer des Données du Partenaire pendant la Période de validité et que les Données du Partenaire ne peuvent pas être récupérées par lui, cette utilisation constitue alors une Instruction pour Google de supprimer des systèmes Google les Données du Partenaire concernées. Google s'engage à respecter cette Instruction dans les meilleurs délais pratiques et raisonnables et sous 180 (cent quatre-vingts) jours au maximum, à moins que la Législation européenne (lorsque la Législation européenne sur la protection des données s'applique) ou la législation en vigueur (lorsque tout autre Droit applicable relatif à la confidentialité s'applique) ne requière le stockage de ces données.

6.2 *Restitution ou suppression à l'expiration de la Période de validité*. Si le Partenaire souhaite conserver des Données du Partenaire après l'expiration de la Période de validité, il peut demander à Google, conformément à la Section 9.1 (Accès ; Rectification ; Limitation du traitement ; Portabilité), de restituer ces données pendant la Période de validité. Le Partenaire demande à Google de supprimer toutes les autres Données du Partenaire (y compris les copies existantes) des systèmes Google à la fin de la Période de validité. À l'issue d'une période de récupération allant jusqu'à 30 (trente) jours après cette date, Google se conformera à cette Instruction dans les meilleurs délais pratiques et raisonnables et sous 180 (cent quatre-vingts) jours au maximum, à moins que la Législation européenne (lorsque la Législation européenne sur la protection des données s'applique) ou la législation en vigueur (lorsque tout autre Droit applicable relatif à la confidentialité s'applique) ne requière le stockage desdites données.

7. Sécurité des données

7.1 *Mesures et contrôles de sécurité, et assistance de Google en matière de sécurité*.

7.1.1 *Mesures de sécurité de Google*. Google s'engage à mettre en œuvre et garder opérationnelles des mesures techniques, organisationnelles et physiques pour protéger les Données du Partenaire contre les destructions, pertes, altérations, divulgations ou accès non autorisés, qu'il s'agisse d'actions accidentelles ou malveillantes, comme décrit dans l'Annexe 2 (Mesures de sécurité) (les « *Mesures de sécurité* »). Les Mesures de sécurité incluent des mesures pour permettre le chiffrement des Données du Partenaire ; pour garantir la confidentialité, l'intégrité, la disponibilité et la résilience continues des systèmes et services de Google ; pour rétablir rapidement l'accès aux Données du Partenaire à la suite d'un incident ; et pour tester régulièrement leur efficacité. Google peut, de temps en temps, mettre à jour les Mesures de sécurité à condition que ces mises à jour n'entraînent pas de réduction substantielle de la sécurité des Services.

7.1.2 *Accès et conformité*. Google s'engage à :

a. n'autoriser ses employés, sous-traitants et Sous-traitants indirects à accéder aux Données du Partenaire que dans la mesure strictement nécessaire pour se conformer aux Instructions ;

b. prendre des mesures raisonnables pour s'assurer que ses employés, sous-traitants et Sous-traitants indirects se conforment aux Mesures de sécurité dans la limite applicable à leur champ de performance ; et

c. s'assurer que toutes les personnes autorisées à traiter les Données du Partenaire se sont engagées à respecter leur caractère confidentiel.

7.1.3 *Contrôles de sécurité supplémentaires*. Google s'engage à rendre disponibles des Contrôles de sécurité supplémentaires dans le but de :

a. permettre au Partenaire de prendre les mesures nécessaires pour sécuriser les Données du Partenaire ; et

b. fournir au Partenaire des informations sur la sécurisation et l'utilisation des Données du Partenaire ainsi que sur l'accès à celles-ci.

7.1.3 *Assistance de Google en matière de sécurité*. Selon la nature du traitement des Données à caractère personnel du Partenaire et selon les informations à sa disposition, Google s'engage à aider le Partenaire à s'assurer qu'il respecte ses obligations (ou les obligations du responsable du traitement concerné si le Partenaire est un sous-traitant) en matière de sécurité et de violation des données à caractère personnel en vertu du Droit applicable relatif à la confidentialité :

a. en mettant en œuvre et en gardant opérationnelles les Mesures de sécurité conformément à la Section 7.1.1 (Mesures de sécurité de Google) ;

b. en mettant à disposition des Contrôles de sécurité supplémentaires conformément à la Section 7.1.3 (Contrôles de sécurité supplémentaires) ;

c. en respectant les conditions de la Section 7.2 (Incidents liés aux données) ;

d. en mettant à disposition la Documentation sur la sécurité conformément à la Section 7.5.1 (Examen de la Documentation sur la sécurité) et en transmettant les informations contenues dans le Contrat (y compris le présent Avenant) ; et

e. si les sous-sections (a) à (d) ci-dessus ne suffisent pas à permettre au Partenaire (ou au responsable du traitement concerné) de respecter lesdites obligations, en offrant au Partenaire une coopération et une assistance supplémentaires raisonnables à sa demande.

7.2 *Incidents liés aux données*.

7.2.1 *Notification d'incident*. Google s'engage à informer rapidement et sans délai indu le Partenaire d'un Incident lié aux données dès qu'il en a connaissance et de prendre rapidement des mesures raisonnables afin de minimiser les dommages et de sécuriser les Données du Partenaire.

7.2.2 *Détails de l'Incident lié aux données*. La notification par Google d'un Incident lié aux données décrit : la nature de l'Incident lié aux données, y compris les ressources du Partenaire qui sont touchées ; les mesures que Google a prises ou compte prendre pour remédier à l'Incident lié aux données et atténuer les risques éventuels ; les éventuelles mesures que Google recommande au Partenaire de prendre afin de remédier à l'Incident lié aux données ; et les coordonnées d'un point de contact pouvant fournir des informations complémentaires. Si les informations susmentionnées ne peuvent pas toutes être fournies en même temps, la première notification par Google doit inclure les informations alors disponibles, les informations restantes devant ensuite être fournies sans délai indu dès qu'elles deviennent disponibles.

7.2.3 *Aucune obligation d'examen des Données du Partenaire par Google*. Google n'est pas tenu d'examiner les Données du Partenaire pour identifier dans celles-ci les informations soumises à des obligations légales.

7.2.4 *Absence de reconnaissance de tort par Google*. La notification par Google d'un Incident lié aux données ou sa réponse à un tel incident conformément à la présente Section 7.2 (Incidents liés aux données) ne saurait être interprétée comme une reconnaissance de tort ou de culpabilité par Google en lien avec l'Incident lié aux données.

7.3 *Responsabilités du Partenaire en matière de sécurité et évaluation de la sécurité*.

7.3.1 *Responsabilités du Partenaire en matière de sécurité*. Sans préjudice des obligations de Google au titre des Sections 7.1 (Mesures et contrôles de sécurité, et assistance de Google en matière de sécurité) et 7.2 (Incidents liés à la sécurité) et des autres sections du Contrat conclu entre Google et le Partenaire, le Partenaire est responsable de toute utilisation des Services, par lui-même et par ses Clients, ainsi que du stockage de toute copie éventuelle des Données du Partenaire, entrepris par lui-même ou par ses Clients, en dehors des systèmes de Google ou des systèmes des Sous-traitants indirects de Google, y compris :

a. l'utilisation des Services et Contrôles de sécurité supplémentaires pour assurer un niveau de sécurité adapté au risque auquel sont exposées les Données du Partenaire ;

b. la sécurisation des identifiants d'authentification de compte, des systèmes et des appareils qu'utilisent le Partenaire et ses Clients pour accéder aux Services ; et

c. la sauvegarde des données du Partenaire, le cas échéant.

7.3.2 *Évaluation de la sécurité par le Partenaire*. Le Partenaire accepte que les Services, Mesures de sécurité, Contrôles de sécurité supplémentaires, et les engagements de Google au titre de cette Section 7 (Sécurité des données) offrent un niveau de sécurité adapté au risque auquel sont exposées les Données du Partenaire (en tenant compte des avancées technologiques, des coûts de mise en œuvre et de la nature, du champ d'application, du contexte et des finalités du traitement des Données du Partenaire ainsi que des risques pour les personnes physiques).

7.4 *Certifications de conformité et Rapports SOC*. Google s'engage à maintenir a minima les évaluations vis-à-vis des normes suivantes pour les Services audités afin de valider l'efficacité continue des Mesures de sécurité :

a. Des certificats pour ISO 27001 et toute certification supplémentaire décrite dans l'Annexe 4 (Produits spécifiques) (les « *Certifications de conformité* ») ; et

b. Des rapports SOC 2 et SOC 3 produits par un Auditeur tiers de Google et mis à jour tous les ans sur la base d'un audit réalisé au moins tous les 12 mois (les « *Rapports SOC* »).

Google peut ajouter des normes à tout moment. Google se réserve le droit de trouver une alternative équivalente ou de niveau supérieur à une Certification de conformité ou à un Rapport SOC.

7.5 *Examens et audits de conformité*.

7.5.1 *Examen de la Documentation sur la sécurité*. Pour démontrer qu'il se conforme à ses obligations en vertu du présent Avenant, Google s'engage à mettre à la disposition du Partenaire la Documentation sur la sécurité pour que le Partenaire puisse l'examiner et, si le Partenaire est un sous-traitant, s'engage à permettre au Partenaire de demander l'accès aux Rapports SOC pour le Client et responsable du traitement concerné conformément à la Section 7.5.3 (Conditions supplémentaires pour les examens et les audits).

7.5.2 *Droits d'audit du Partenaire*.

a. *Audit par le Partenaire*. Si le Droit applicable relatif à la confidentialité l'exige, Google s'engage à autoriser le Partenaire ou un auditeur indépendant désigné par le Partenaire à conduire des audits (y compris des inspections) pour vérifier que Google se conforme à ses obligations en vertu du présent Avenant, conformément à la Section 7.5.3 (Conditions supplémentaires pour les examens et les audits). Google s'engage à faire preuve lors des audits d'une coopération raisonnable avec le Partenaire ou son auditeur, comme décrit dans la Section 7.5 (Examens et audits de conformité).

b. *Examen indépendant par le Partenaire*. Le Partenaire peut conduire un audit afin de vérifier que Google se conforme à ses obligations vis-à-vis du présent Avenant en examinant la Documentation sur la sécurité (qui reflète le résultat des audits conduits par l'auditeur tiers de Google).

7.5.3 *Conditions supplémentaires pour les examens et les audits*.

a. Le Partenaire doit contacter l'équipe Google chargée de la protection des données dans le cloud pour demander :

i. l'accès aux Rapports SOC pour un responsable du traitement concerné en vertu de la Section 7.5.1 (Examen de la Documentation sur la sécurité) ; ou

ii. un audit en vertu de la Section 7.5.2(a) (Audit par le Partenaire).

b. À la suite d'une demande formulée par le Partenaire en vertu de la Section 7.5.3(a), Google et le Partenaire s'engagent à discuter et à convenir par avance :

i. des contrôles de sécurité et de confidentialité applicables à tout accès aux Rapports SOC par un responsable du traitement concerné en vertu de la Section 7.5.1 (Examen de la Documentation sur la sécurité) ; et

ii. de la date de début, du champ d'application et de la durée raisonnables de tout audit en vertu de la Section 7.5.2(a) (Audit par le Partenaire), ainsi que des contrôles de confidentialité et de sécurité applicables.

c. Google se réserve le droit de facturer des frais (basés sur les coûts raisonnables de Google) pour tout audit effectué en vertu de la Section 7.5.2(a) (Audit par le Partenaire). Google s'engage à fournir au Partenaire avant ledit audit des détails supplémentaires sur les frais applicables ainsi que sur la façon dont ils ont été calculés. Le Partenaire est responsable du paiement des frais facturés par tout auditeur qu'il a désigné pour effectuer l'audit.

d. Google peut s'opposer par écrit au fait qu'un auditeur désigné par le Partenaire effectue un audit conformément à la Section 7.5.2(a) (Audit par le Partenaire) si l'auditeur, de l'avis raisonnable de Google, n'est pas suffisamment compétent ou indépendant, est un concurrent de Google ou n'est manifestement pas un acteur approprié. Dans le cas d'une telle objection par Google, le Partenaire doit désigner un autre auditeur ou effectuer l'audit lui-même.

e. Toute demande d'accès à des Rapports SOC pour un responsable du traitement concerné ou pour des audits, formulée par le Partenaire en vertu de l'Annexe 3 (Droits spécifiques relatifs à la confidentialité) ou de l'Annexe 4 (Produits spécifiques), sera également régie par les modalités de la présente Section 7.5.3 (Conditions supplémentaires pour les examens et les audits).

8. Évaluations d'impact et consultations

Selon la nature du traitement et selon les informations à sa disposition, Google s'engage à aider le Partenaire à s'assurer qu'il respecte ses obligations (ou les obligations du responsable du traitement concerné si le Partenaire est un sous-traitant) concernant les évaluations liées à la protection des données, les évaluations des risques, les consultations réglementaires antérieures ou les procédures équivalentes en vertu du Droit applicable relatif à la confidentialité :

a. en mettant à disposition des Contrôles de sécurité supplémentaires conformément à la Section 7.1.3 (Contrôles de sécurité supplémentaires) ainsi que la Documentation sur la sécurité conformément à la Section 7.5.1 (Examen de la Documentation sur la sécurité) ;

b. en fournissant les informations contenues dans le Contrat (y compris le présent Avenant) ; et

c. si les sous-sections (a) et (b) ci-dessus ne suffisent pas à permettre au Partenaire (ou responsable du traitement concerné) de respecter lesdites obligations, en offrant au Partenaire une coopération et une assistance supplémentaires raisonnables à sa demande.

9. Accès, etc. ; Droits de la personne concernée ; Exportation des données

9.1 *Accès ; Rectification ; Limitation du traitement ; Portabilité*. Pendant toute la Période de validité des présentes, Google s'engage, tout en respectant les fonctionnalités des Services, à permettre au Partenaire d'accéder aux données le concernant, de les rectifier et d'en limiter le traitement, y compris via la fonctionnalité de suppression fournie par Google telle que décrite à la Section 6.1 (Suppression par le Partenaire), ainsi que d'exporter les données du Partenaire. Si le Partenaire constate que des Données à caractère personnel du Partenaire sont inexactes ou obsolètes, il lui revient d'utiliser la fonctionnalité appropriée pour rectifier ou supprimer ces données lorsque le Droit applicable relatif à la confidentialité l'exige.

9.2 *Demandes des personnes concernées*.

9.2.1 *Responsabilité vis-à-vis des demandes*. Si, pendant la Période de validité des présentes, l'équipe Google chargée de la protection des données dans le cloud reçoit une demande d'une personne concernée au sujet des Données à caractère personnel du Partenaire dans laquelle elle identifie le Partenaire, Google s'engage à :

a. inviter la personne concernée à envoyer sa demande au Partenaire ;

b. en notifier le Partenaire sans délai ; et

c. ne pas répondre à la demande de ladite personne concernée sans l'autorisation du Partenaire.

Le Partenaire se chargera de répondre à la demande, en utilisant le cas échéant la fonctionnalité des Services.

9.2.2 *Assistance de Google pour traiter les demandes des personnes concernées*. Selon la nature du traitement des Données à caractère personnel du Partenaire, Google s'engage à aider le Partenaire à remplir ses obligations en vertu du Droit applicable relatif à la confidentialité (ou les obligations du responsable du traitement concerné si le Partenaire est un sous-traitant) quant à l'apport d'une réponse aux demandes de personnes concernées cherchant à exercer leurs droits. Google :

a. mettra à disposition des Contrôles de sécurité supplémentaires conformément à la Section 7.1.3 (Contrôles de sécurité supplémentaires) ;

b. se conformera aux Sections 9.1 (Accès ; Rectification ; Limitation du traitement ; Portabilité) et 9.2.1 (Responsabilité vis-à-vis des demandes) ; et

c. si les sous-sections (a) et (b) ci-dessus ne suffisent pas à permettre au Partenaire (ou responsable du traitement concerné) de respecter lesdites obligations, offrira au Partenaire une coopération et une assistance supplémentaires raisonnables à sa demande.

10. Emplacements de traitement des données

10.1 *Installations de stockage et de traitement des données*. Sous réserve des engagements de Google en matière de localisation des données et en vertu des Conditions spécifiques des Services, ainsi qu'en matière de transfert des données en vertu de l'Annexe 3 (Droits spécifiques relatifs à la confidentialité), les données du Partenaire peuvent être traitées, le cas échéant, dans n'importe quel pays où Google ou ses Sous-traitants indirects disposent d'installations.

10.2 *Informations sur les centres de données*. Les emplacements des centres de données Google sont décrits dans l'Annexe 4 (Produits spécifiques).

11. Sous-traitants indirects

11.1 *Autorisation d'engagement de Sous-traitants indirects*. Le Partenaire autorise expressément Google à engager en tant que Sous-traitants indirects les entités mentionnées, tel que décrit à la Section 11.2 (Informations sur les Sous-traitants indirects), à compter de la Date d'entrée en vigueur de l'Avenant. De plus, sans porter préjudice à la Section 11.4 (Possibilité de s'opposer à des Sous-traitants indirects), le Partenaire autorise de façon générale Google à engager d'autres tiers en tant que Sous-traitants indirects (« *Nouveaux Sous-traitants indirects* »).

11.2 *Informations sur les Sous-traitants indirects*. Les noms, sites d'implantation et activités des Sous-traitants indirects sont décrits dans l'Annexe 4 (Produits spécifiques).

11.3 *Conditions requises pour l'engagement de Sous-traitants indirects*. Lors de l'engagement d'un Sous-traitant, Google doit :

a. s'assurer par un contrat écrit que :

i. le Sous-traitant indirect n'accède aux données du Partenaire et ne les utilise qu'aux fins requises pour satisfaire aux obligations qui lui sont sous-traitées, et conformément au Contrat (y compris au présent Avenant) ; et

ii. lorsque les Droits applicables relatifs à la confidentialité l'exigent, les obligations liées à la protection des données décrites dans les présentes sont imposées au Sous-traitant indirect (tel que décrit dans l'Annexe 3 (Droits spécifiques relatifs à la confidentialité)) ; et

b. demeurer entièrement responsable de toutes les obligations déléguées au Sous-traitant indirect, et de l'ensemble des actes et manquements de celui-ci.

11.4 *Possibilité de s'opposer à des Sous-traitants indirects*.

a. Lorsque Google engage un nouveau Sous-traitant indirect pendant la Période de validité, Google s'engage à informer le Partenaire dudit engagement (y compris du nom, de l'emplacement et des activités du nouveau Sous-traitant indirect) au moins 30 (trente) jours avant que le nouveau Sous-traitant indirect ne commence à traiter les données du Partenaire.

b. Sous un délai de 90 (quatre-vingt-dix) jours après avoir été informé de l'engagement d'un nouveau Sous-traitant indirect, le Partenaire peut s'y opposer en résiliant immédiatement le Contrat pour convenance :

i. conformément à la clause de résiliation pour convenance contenue dans ledit Contrat ; ou

ii. en l'absence d'une telle clause, en en informant Google.

12. Équipe chargée de la protection des données dans le cloud ; Archives de traitement

12.1 *Équipe chargée de la protection des données dans le cloud*. L'équipe Google chargée de la protection des données dans le cloud s'engage à fournir une assistance rapide et raisonnable à toute demande formulée par le Partenaire en lien avec le traitement des données du Partenaire en vertu du Contrat. Elle peut être contactée comme décrit dans la Section Avis du Contrat ou dans l'Annexe 4 (Produits spécifiques).

12.2 *Archives de traitement de Google*. Google s'engage à conserver toute documentation appropriée concernant ses activités de traitement conformément au Droit applicable relatif à la confidentialité. Dans la mesure où le Droit applicable relatif à la confidentialité exige de Google qu'il collecte et conserve certaines informations concernant le Partenaire ou ses Clients, le Partenaire s'engage à utiliser la console d'administration ou d'autres moyen identifiés dans l'Annexe 4 (Produits spécifiques) pour fournir lesdites informations et les garder exactes et à jour. Google peut fournir lesdites informations à des organismes de réglementation compétents, y compris à une autorité de contrôle, si le Droit applicable relatif à la confidentialité l'exige.

12.3 *Demandes du responsable du traitement*. Si, pendant la Période de validité des présentes, l'équipe Google chargée de la protection des données dans le cloud reçoit une demande ou instruction de la part d'un tiers se présentant comme un responsable du traitement des Données à caractère personnel du Partenaire, Google invitera le tiers à contacter le Partenaire.

13. Avis

Tout avis envoyé en vertu du présent Avenant (y compris toute notification d'Incident lié aux données) sera envoyé à l'Adresse courriel de notification. Le Partenaire doit vérifier dans la console d'administration que son Adresse courriel de notification est toujours d'actualité et valide, ou informer Google de toute modification la concernant.

14. Interprétation

14.1 *Priorité*. En cas de conflit entre :

a. l'Annexe 3 (Droits spécifiques relatifs à la confidentialité) et le reste de l'Avenant (y compris l'Annexe 4 (Produits spécifiques)), l'Annexe 3 prévaut ; et

b. l'Annexe 4 (Produits spécifiques) et le reste de l'Avenant (à l'exception de l'Annexe 3), l'Annexe 4 prévaut ; et

c. les présentes et le reste du Contrat, les présentes prévalent.

14.2 *Références à d'autres sections*. Sauf indication contraire, les références à d'autres sections apparaissant dans une Annexe du présent Avenant renvoient aux sections des Conditions générales de l'Avenant.

14.3 *Clients*. Par souci de clarification, les Clients ne sont pas à considérer comme des tiers bénéficiaires du présent Avenant.

Annexe 1 : Objet et détails du traitement des données

Objet

Fourniture des Services et des SAT au Partenaire par Google.

Durée du traitement

Correspond à la Période de validité, plus la période allant de la fin de la Période de validité à la suppression de toutes les données du partenaire par Google conformément aux présentes.

Nature et finalité du traitement

Google s'engage à traiter les Données à caractère personnel du Partenaire pour assurer la fourniture des Services et des SAT au Partenaire conformément aux présentes.

Catégories de données

Données concernant des personnes physiques et fournies à Google via les Services, par le (ou sous les instructions du) Partenaire ou ses Clients ou par les Utilisateurs finaux du Partenaire.

Personnes concernées

Les Personnes concernées désignent les personnes physiques à propos desquelles des données sont fournies à Google via les Services par le (ou sous les instructions du) Partenaire ou ses Clients ou par les Utilisateurs finaux du Partenaire.

Annexe 2 : Mesures de sécurité

À compter de la Date d'entrée en vigueur de l'Avenant, Google s'engage à mettre en œuvre et à garder opérationnelles les Mesures de sécurité définies dans la présente Annexe 2.

1. Centre de données et sécurité du réseau

(a) Centres de données.

Infrastructure. Google gère des centres de données répartis dans différentes zones géographiques. Google stocke toutes les données de production dans des centres de données physiquement sécurisés.

Redondance. Les systèmes d'infrastructure ont été conçus pour supprimer les points de défaillance uniques et minimiser l'impact des risques environnementaux prévisibles. Cette redondance repose entre autres sur des circuits doubles, des commutateurs, des réseaux et d'autres appareils nécessaires.

Les Services sont conçus de façon à permettre à Google d'effectuer certains types de tâches 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 des équipements des centres de données est planifiée selon un processus standard de mise en œuvre des changements, conformément aux procédures documentées.

Alimentation. Les systèmes d'alimentation électrique des centres de données sont conçus pour être redondants et pour que leur maintenance puisse être assurée sans interruption de fonctionnement, 24h/24 et 7j/7. Dans la plupart des cas, une source de courant principale et une source alternative de capacités égales sont prévues pour les composants critiques de l'infrastructure du centre de données. L'alimentation de secours est assurée par différents mécanismes, par exemple des batteries d'alimentation sans interruption (de type onduleur) qui fournissent une protection électrique fiable pour tous les types de perturbations (tension instable, coupures de courant, surtensions, sous-tensions et conditions de fréquences hors tolérance) affectant les dispositifs de fourniture d'électricité. En cas de coupure de courant sur le réseau principal, l'alimentation de secours est conçue pour fournir une source de courant transitoire au centre de données, à pleine capacité, pendant une durée maximale de 10 minutes, jusqu'à ce que les générateurs de secours prennent le relais. Les générateurs de secours sont capables de démarrer automatiquement en quelques secondes afin de fournir suffisamment de courant électrique de secours pour faire fonctionner le centre de données à pleine capacité, en général pendant plusieurs jours.

Systèmes d'exploitation serveur. Les serveurs Google utilisent une implémentation Linux personnalisée pour l'environnement d'application. Les données sont stockées à l'aide d'algorithmes propriétaires qui permettent de renforcer la redondance et la sécurité des données.

Qualité du code. Google applique un processus de revue de code afin d'accroître la sécurité du code utilisé pour fournir les Services et d'améliorer les produits de sécurité dans les environnements de production.

Continuité des activités. Google a conçu des plans de continuité des activités et des programmes de reprise après sinistre qui sont planifiés et testés régulièrement.

(*b) Réseaux et transmission*.

Transmission des données. En règle générale, les centres de données sont reliés entre eux via des connexions privées à haut débit, ce qui permet de garantir un transfert sûr et rapide des données d'un centre à l'autre. Le but est d'empêcher la lecture, la copie, la modification ou la suppression non autorisées des données au cours de leur transfert ou de leur transport par voie électronique, ou encore lors de leur enregistrement sur des supports de stockage de données. 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 à ses systèmes externes des technologies dédiées à ces menaces.

Détection des intrusions. La détection des intrusions vise à fournir des insights sur les activités en cours liées à des attaques et sur la façon de réagir aux incidents. La détection des intrusions de Google implique : (i) le contrôle rigoureux de la taille et de la composition de la surface d'attaque de Google via des mesures préventives ; (ii) la mise en place de contrôles de détection intelligents aux points d'entrées des données ; et (iii) l'utilisation de technologies qui résolvent automatiquement les problèmes liés à certaines situations dangereuses.

Réponse aux 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 propose le chiffrement HTTPS (également appelé connexion SSL ou TLS). Les serveurs Google acceptent 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) contribuent à protéger le trafic et à minimiser l'impact d'une clé compromise ou d'une avancée en matière de cryptographie.

2. Contrôle sur site et contrôle d'accès.

(a) Contrôles sur site.

Gestion de la sécurité des centres de données sur site. La sécurité des centres de données de Google est gérée par une équipe sur site. L'objectif est de garantir le fonctionnement de toutes les fonctions de sécurité physiques des centres de données, 24h/24 et 7j/7. Le personnel responsable de la gestion de la sécurité sur site contrôle un réseau de caméras de surveillance en circuit fermé, ainsi que tous les systèmes d'alarme. Il effectue régulièrement des patrouilles internes et externes sur le site des centres de données.

Procédures d'accès aux centres de données. Google applique des procédures d'accès formelles pour autoriser l'accès physique à ses centres de données. Les centres de données sont hébergés dans des locaux nécessitant une carte d'accès électronique. Ils sont équipés d'alarmes reliées au centre de gestion de la sécurité sur site. Toute personne souhaitant pénétrer dans le centre de données doit s'identifier et présenter une pièce d'identité au personnel gérant la sécurité du site. Seuls les employés, les contractants et les visiteurs autorisés sont admis dans les centres de données. Les employés et les contractants autorisés sont les seules personnes en droit de demander un accès par carte électronique à ces locaux. Les demandes d'accès par carte électronique doivent être faites par courriel et validées par le responsable du demandeur et par le directeur du centre de données. Toutes les autres personnes demandant un accès provisoire au centre de données doivent : (i) obtenir à l'avance l'autorisation des responsables du centre de données pour le centre de données lui-même et les zones où elles souhaitent se rendre ; (ii) se présenter auprès de l'équipe de gestion de la sécurité sur site ; et (iii) remplir un registre officiel d'accès au centre de données qui les identifie comme visiteurs autorisés.

Dispositifs de sécurité des centres de données sur site. Les centres de données de Google utilisent un système de contrôle des accès à double authentification lié à une alarme système. Le système de contrôle des accès surveille et enregistre la carte électronique de chaque personne, ainsi que les franchissements des portes du périmètre et l'accès aux zones d'expédition et de réception, ainsi qu'à d'autres zones critiques. Les activités non autorisées et les tentatives d'accès non abouties sont enregistrées par le système de contrôle des accès, puis examinées, selon les cas. Au niveau de la

gestion des activités commerciales et des centres de données, l'accès est limité selon les zones et les responsabilités professionnelles de la personne concernée. Les portes coupe-feu des centres de données sont équipées d'alarmes. Des caméras de surveillance sont installées à l'intérieur et à l'extérieur des centres de données. Elles sont positionnées de façon à couvrir les zones stratégiques, parmi lesquelles le périmètre du site, les portes du bâtiment du centre de données et les zones d'expédition et de réception. Le personnel chargé de la gestion de la sécurité sur site est responsable des équipements de contrôle, d'enregistrement et de surveillance CCTV. Des câbles sécurisés sont installés dans tout le périmètre des centres de données pour connecter les équipements de vidéosurveillance. Les caméras enregistrent les images du site grâce à des enregistreurs vidéo numériques 24h/24, 7j/7. Les enregistrements de vidéosurveillance sont conservés pendant 30 jours au maximum selon les activités.

(b) Contrôle des accès.

Personnel de sécurité des infrastructures. Google a mis en place et applique des règles de sécurité pour son personnel, lequel doit obligatoirement suivre une formation à la sécurité dans le cadre de sa formation globale. Le personnel de sécurité des infrastructures de Google est chargé de la surveillance permanente des infrastructures de sécurité de Google, de la vérification des Services et de la résolution des incidents de sécurité.

Contrôle des accès et gestion des droits. Les administrateurs du Partenaire et les Utilisateurs finaux du Partenaire doivent s'authentifier par l'intermédiaire d'un système d'authentification central ou d'authentification unique afin d'utiliser les Services.

Processus et règles internes d'accès aux données – Règles d'accès. Les processus et règles internes d'accès aux données de Google sont destinés à empêcher les personnes et systèmes non autorisés d'accéder aux systèmes utilisés pour le traitement des Données du Partenaire. Google conçoit ses systèmes de façon à (i) ne permettre qu'aux personnes autorisées d'accéder aux données auxquelles elles sont en droit d'accéder ; et (ii) empêcher la lecture, la copie, l'altération ou la suppression des Données du Partenaire sans autorisation lors de leur traitement, en cours d'utilisation ou après leur enregistrement. Les systèmes permettent de détecter les accès inappropriés. Google utilise un système de gestion des accès centralisé pour contrôler l'accès du personnel aux serveurs de production et n'autorise l'accès qu'à un nombre limité d'employés. Les systèmes d'authentification et d'autorisation de Google reposent sur des certificats et clés de sécurité SSH. Ils sont conçus pour fournir à Google des mécanismes d'accès sécurisés et flexibles. Ces mécanismes n'octroient des droits d'accès aux hôtes des sites, aux journaux, aux données et aux informations de configuration qu'au personnel dûment autorisé. Google requiert l'utilisation d'ID utilisateur uniques, de mots de passe sécurisés, de l'authentification à deux facteurs et de listes d'accès faisant l'objet d'un suivi attentif, de façon à réduire les risques d'utilisation abusive des comptes. L'octroi et la modification des droits d'accès sont basés sur les responsabilités professionnelles du personnel autorisé, les prérequis nécessaires à l'exécution des tâches autorisées, et le principe du 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 flux de travail 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), des stratégies de mot de passe qui respectent

au moins les pratiques standards du secteur sont appliquées. Ces pratiques standards incluent entre autres les restrictions relatives à la réutilisation des mots de passe et à leur sécurité minimale. Pour l'accès aux informations extrêmement sensibles (données de carte de crédit, par exemple), Google utilise des jetons matériels.

3. Données

(a) *Stockage, isolation et journalisation des données*. Google stocke les données dans un environnement mutualisé, sur des serveurs qui lui appartiennent. Sauf instructions contraires (comme la sélection d'un emplacement pour les données, par exemple), Google réplique les données du Partenaire sur plusieurs centres de données dispersés géographiquement. Google applique également une isolation logique pour les Données du Partenaire. Le Partenaire se voit confier le contrôle de certaines règles de partage des données. Lesdites règles, conformément aux fonctionnalités des Services, permettent au Partenaire de déterminer les paramètres de partage de produit qui s'appliquent aux Utilisateurs finaux du Partenaire pour des besoins particuliers. Le Partenaire peut choisir d'utiliser la fonctionnalité de journalisation fournie par Google via les Services.

(b) *Disques mis hors service et règlement d'effacement des disques*. Les disques contenant des données peuvent présenter 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 (le « Règlement d'effacement des disques ») avant de quitter les locaux de Google en vue de sa réutilisation ou de sa destruction. Les Disques mis hors service sont effacés selon un processus en plusieurs étapes, et l'effacement est validé 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. Chacune des installations est contrôlée régulièrement afin de vérifier qu'elle respecte le Règlement d'effacement des disques.

4. Personnel de Google et sécurité des données

Le personnel de Google est tenu de se comporter de manière conforme aux directives de l'entreprise en matière de confidentialité, d'éthique commerciale, d'utilisation adéquate et de normes professionnelles. Google effectue des vérifications raisonnables et appropriées des antécédents, dans la limite autorisée par la loi et conformément à la législation du travail et aux règlements statutaires en vigueur localement.

Le personnel de Google doit respecter un accord de confidentialité ainsi que les règles de Google concernant la confidentialité, dont il doit par ailleurs accuser réception. Il reçoit aussi une formation à la sécurité. Le personnel chargé de manipuler les Données du Partenaire doit en outre se soumettre à des exigences supplémentaires adaptées à son rôle (ex. certifications). Le personnel de Google n'est pas habilité à traiter les Données du Partenaire sans autorisation.

5. Sous-traitants et sécurité des données

Avant d'engager des Sous-traitants, 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 l'accès aux données qui leur est accordé 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 indirect, et sous réserve des exigences décrites à la Section 11.3 (Conditions requises pour l'engagement de Sous-traitants indirects), celui-ci est tenu d'accepter les conditions contractuelles appropriées en termes de sécurité et de confidentialité.

Annexe 3 : Droits spécifiques relatifs à la confidentialité

Les conditions décrites dans chaque sous-section de la présente Annexe 3 ne s'appliquent que lorsque le droit correspondant s'applique au traitement des Données à caractère personnel du Partenaire.

Législation européenne sur la protection des données

1. Définitions supplémentaires.

- « *Pays approprié* » désigne :

  (a) lorsque les données sont traitées conformément au RGPD de l'UE : l'Espace économique européen, ou un pays ou territoire reconnu comme garantissant une protection appropriée en vertu du RGPD de l'UE ;

  (b) lorsque les données sont traitées conformément au RGPD du Royaume-Uni : le Royaume-Uni, ou un pays ou territoire reconnu comme garantissant une protection appropriée en vertu du RGPD du Royaume-Uni et du Data Protection Act 2018 ; ou

  (c) lorsque les données sont traitées conformément à la LPD de la Suisse : la Suisse, ou un pays ou territoire qui : (i) figure dans la liste des États dont la législation garantit une protection appropriée, comme publié par le Préposé fédéral suisse à la protection des données et à la transparence, le cas échéant ; ou (ii) est reconnu par le Conseil fédéral suisse comme offrant une protection appropriée en vertu de la LPD de la Suisse ;

  dans chaque cas, un pays qui offre plus qu'un simple cadre facultatif de protection des données.

- « *Solution de transfert alternative* » désigne une solution, autre que les clauses contractuelles types (CCT), qui permet le transfert légal de données à caractère personnel vers un pays tiers, conformément à la Législation européenne sur la protection des données. Il peut s'agir par exemple d'un cadre de protection des données dont on reconnaît que les entités participantes fournissent une protection adéquate.

- « *CCT du Partenaire* » désigne les CCT (responsable du traitement à sous-traitant), les CCT (sous-traitant à sous-traitant) ou les CCT (sous-traitant à responsable du traitement), selon le cas.

- « *CCT* » désigne les CCT du Partenaire ou les CCT (sous-traitant à sous-traitant, exportateur Google), selon le cas.
- « *CCT (responsable du traitement à sous-traitant)* » désigne les conditions publiées sur la page https://cloud.google.com/terms/sccs/eu-c2p
- « *CCT (sous-traitant à responsable du traitement)* » désigne les conditions publiées sur la page https://cloud.google.com/terms/sccs/eu-p2c
- « *CCT (sous-traitant à sous-traitant)* » désigne les conditions publiées sur la page https://cloud.google.com/terms/sccs/eu-p2p
- « *CCT (sous-traitant à sous-traitant, exportateur Google)* » désigne les conditions publiées sur la page https://cloud.google.com/terms/sccs/eu-p2p-google-exporter

2. Avis d'Instruction. Sans préjudice des obligations de Google au titre de la Section 5.2 (Conformité avec les Instructions du Partenaire) ni à tout autre droit ou obligation des parties en vertu du Contrat, Google s'engage à informer immédiatement le Partenaire s'il estime :

a. que la Législation européenne empêche Google de se conformer à une Instruction ;

b. qu'une Instruction va à l'encontre de la Législation européenne sur la protection des données ; ou

c. que Google ne peut pas se conformer à une Instruction, dans chaque cas sous réserve que la Législation européenne autorise l'envoi d'un tel avis.

Si le Partenaire est un sous-traitant, il s'engage à transmettre immédiatement au responsable du traitement concerné tout avis provenant de Google tel que décrit dans la présente Section.

3. Droits d'audit du Partenaire. Google s'engage à permettre au Partenaire ou à un auditeur indépendant désigné par celui-ci d'effectuer des audits (y compris des inspections), comme décrit à la Section 7.5.2(a) (Audit par le Partenaire). Pendant ledit audit, Google s'engage à mettre à disposition toutes les informations nécessaires permettant de démontrer sa conformité vis-à-vis de ses obligations au titre des présentes et de contribuer à l'audit comme décrit à la Section 7.5 (Examens et Audits de conformité) et dans la présente section.

4. Transferts de données.

5.1 *Transferts limités.* Les parties reconnaissent que la Législation européenne sur la protection des données n'exige aucune CCT ni Solution de transfert alternative en vue du traitement des Données à caractère personnel du Partenaire dans un Pays approprié ou de leur transfert vers un Pays approprié. Si les Données à caractère personnel du Partenaire sont transférées vers un autre pays et que la Législation européenne sur la protection des données s'applique aux transferts (tel que certifié par le Partenaire au titre de la Section 4.2 (Certification par les Partenaires basés hors de la région EMEA) des présentes conditions concernant la Législation européenne sur la protection des données, si son adresse de facturation se situe en dehors de la région EMEA) (« *Transferts limités* ») :

a. si Google a adopté une Solution de transfert alternative pour les Transferts limités, il s'engage à informer le Partenaire de la solution concernée et de veiller à ce que lesdits Transferts limités soient effectués conformément à cette dernière ; ou

b. si Google n'a pas adopté de Solution de transfert alternative pour les Transferts limités, ou qu'il indique au Partenaire qu'il a annulé l'adoption d'une Solution de transfert alternative pour les Transferts limités (sans adopter de Solution de transfert alternative de remplacement) :

i. si l'adresse de Google se situe dans un Pays approprié :

A. les CCT (sous-traitant à sous-traitant, exportateur Google) s'appliquent aux Transferts limités entre Google et les Sous-traitants indirects ; et

B. de plus, si l'adresse de facturation du Partenaire ne se situe pas dans un Pays approprié, les CCT (sous-traitant à responsable du traitement) s'appliquent (que le Partenaire soit un responsable du traitement ou un sous-traitant) auxdits Transferts limités entre Google et le Partenaire ; ou

ii. si l'adresse de Google ne se situe pas dans un Pays approprié, les CCT (responsable du traitement à sous-traitant) ou les CCT (sous-traitant à sous-traitant) s'appliquent (selon que le Partenaire est un responsable du traitement ou un sous-traitant) auxdits Transferts limités entre Google et le Partenaire.

4.2 *Certification par les Partenaires basés hors de la région EMEA*. Si l'adresse de facturation du Partenaire se situe en dehors de la région EMEA et que le traitement des Données à caractère personnel du Partenaire est régi par la Législation européenne sur la protection des données, le Partenaire s'engage, sauf indication contraire dans l'Annexe 4 (Produits spécifiques) du présent Avenant, à attester de ce statut et à identifier son Autorité de contrôle compétente via la Console d'administration pour les Services concernés.

4.3 *Informations sur les Transferts limités*. Google s'engage à fournir au Partenaire des informations pertinentes concernant les Transferts limités, Contrôles de sécurité supplémentaires et autres mesures de protection complémentaires :

a. comme décrit à la Section 7.5.1 (Examen de la Documentation sur la sécurité) ;

b. à tout emplacement supplémentaire décrit dans l'Annexe 4 (Produits spécifiques) ; et

c. concernant l'adoption par Google d'une Solution de transfert alternative, à l'adresse https://cloud.google.com/terms/alternative-transfer-solution.

4.4 *Audits des CCT*. Si les CCT du Partenaire s'appliquent tel que décrit à la Section 4.1 (Transferts limités) des présentes conditions concernant la Législation européenne sur la protection des données, et conformément à la Section 7.5.3 (Conditions supplémentaires pour les examens et les audits), Google autorise le Partenaire (ou un auditeur indépendant désigné par le Partenaire) à effectuer des audits comme décrit dans lesdites CCT et, pendant un audit, s'engage à mettre à disposition toutes les informations requises par lesdites CCT.

4.5 *Avis concernant les CCT*. Le Partenaire s'engage à transmettre rapidement et sans délai indu au responsable du traitement concerné tout avis concernant les CCT.

4.6 *Résiliation liée à un risque pour le transfert de données*. Si, sur la base de son utilisation actuelle ou prévue des Services, le Partenaire conclut que les Données à caractère personnel du Partenaire transférées ne bénéficient pas de garanties appropriées, il peut résilier immédiatement le Contrat conformément à la clause de résiliation pour convenance dudit Contrat ou, en l'absence d'une telle provision, en en informant Google.

4.7 *Aucune intention de modification des CCT*. Rien dans le Contrat (y compris le présent Avenant) n'a pour intention de modifier ou de contredire quelque CCT que ce soit, ni de porter préjudice aux libertés et droits fondamentaux des personnes concernées accordés par la Législation européenne sur la protection des données.

4.8 *Priorité des CCT*. En cas de conflit ou d'incohérence entre les CCT du Partenaire (qui sont intégrées par référence dans les présentes) et le reste du Contrat (y compris le présent Avenant), les CCT du Partenaire prévalent.

5. Conditions requises pour engager des Sous-traitants indirects. La Législation européenne sur la protection des données exige que Google veille, au moyen d'un contrat écrit, à ce que les obligations en matière de protection des données énoncées dans les présentes, telles que visées par l'Article 28(3) du RGPD, le cas échéant, soient imposées à tout Sous-traitant indirect engagé par Google.

CCPA

1. Définitions supplémentaires.

- « *CCPA* » désigne la loi de 2018 sur la protection des données personnelles du consommateur en Californie (California Consumer Privacy Act 2018), telle qu'amendée par la loi de 2020 sur les droits au respect de la confidentialité en Californie (California Privacy Rights Act), avec toutes les dispositions d'application.

- Les « *Données à caractère personnel du Partenaire* » incluent les « informations personnelles ».

- Les termes « entreprise », « finalité commerciale », « consommateur », « informations personnelles », « traitement », « vente », « vendre », « fournisseur de services » et « partager » ont la signification qui leur est attribuée dans le CCPA.

2. Interdictions. Concernant le traitement des Données à caractère personnel du Partenaire conformément au CCPA et sans préjudice des obligations de Google au titre de la Section 5.2 (Conformité avec les Instructions du Partenaire), Google s'engage, sauf si le CCPA le permet, à :

a. ne pas vendre ni partager les Données à caractère personnel du Partenaire ;

b. ne pas conserver, utiliser ni divulguer les Données à caractère personnel du Partenaire :

i. sauf pour une finalité commerciale en vertu du CCPA, au nom du Partenaire et dans le but spécifique de fournir les Services et CCT ; ou

ii. en dehors de la relation commerciale directe entre Google et le Partenaire ; ou

c. ne pas combiner ni mettre à jour les Données à caractère personnel du Partenaire avec des informations personnelles reçues de la part d'un tiers ou en son nom, ou collectées dans le cadre de ses propres interactions avec le consommateur.

3. Conformité. Sans préjudice de ses obligations en vertu de la Section 5.2 (Conformité avec les Instructions du Partenaire) ni de tout autre droit ou obligation de quelconque partie soumise au Contrat, Google s'engage, sauf si le droit applicable le lui interdit, à informer le Partenaire s'il estime ne pas être en mesure de satisfaire à ses obligations au titre du CCPA.

4. Intervention du Partenaire. Si Google informe le Partenaire d'une utilisation non autorisée des Données à caractère personnel du Partenaire, y compris au titre de la Section 3 (Conformité) de la présente sous-section ou de la Section 7.2.1 (Notification de l'incident), le Partenaire peut entreprendre des actions raisonnables et appropriées pour mettre fin ou remédier à ladite utilisation non autorisée :

a. en prenant les mesures recommandées par Google conformément à la Section 7.2.2 (Détails de l'incident lié aux données), le cas échéant ; ou

b. en exerçant ses droits au titre de la Section 7.5.2(a) (Audit par le Partenaire) ou 9.1 (Accès ; Rectification ; Limitation du traitement ; Portabilité).

Turquie

1. Définitions supplémentaires.

- « *Législation turque sur la protection des données* » désigne la loi turque n° 6698 du 7 avril 2016 sur la protection des données à caractère personnel.
- « *Autorité turque chargée de la protection des données à caractère personnel* » désigne le Kişisel Verileri Koruma Kurumu.
- « *CCT turques* » désigne les clauses contractuelles types prévues par la Législation turque sur la protection des données.

2. Transferts de données.

2.1 *Conditions supplémentaires.* Si l'adresse de facturation du Partenaire se situe en Turquie et que Google soumet à l'acceptation du Partenaire des conditions supplémentaires facultatives (y compris des CCT turques) en lien avec les transferts de Données à caractère personnel du Partenaire en vertu de la Législation turque sur la protection des données, lesdites conditions viennent s'ajouter aux présentes à compter de la date à laquelle elles ont été présentées à l'Autorité turque chargée de la protection des données à caractère personnel, conformément à la Section 2.2 (Notification à l'Autorité compétente) ci-dessous, comme attesté par le Partenaire auprès de Google.

2.2 *Notification à l'Autorité compétente*. Si le Partenaire signe des CCT turques au titre de la présente Section 2 (Transferts de données), il doit informer l'Autorité turque chargée de la protection des données à caractère personnel de son utilisation de CCT turques dans un délai de cinq (5) jours ouvrés après signature des CCT turques, tel que l'exige la Législation turque sur la protection des données.

2.3 *Audit des CCT*. Si le Partenaire signe des CCT turques au titre de la présente Section 2 (Transferts de données), Google autorise le Partenaire (ou un auditeur indépendant désigné par ce dernier) à effectuer des audits tels que décrits dans lesdites CCT et, pendant un audit, s'engage à mettre à disposition toutes les informations requises par lesdites CCT, dans les deux cas conformément à la Section 7.5.3 (Conditions supplémentaires pour les examens et les audits).

2.4 *Résiliation liée à un risque pour le transfert de données*. Si, sur la base de son utilisation actuelle ou prévue des Services, le Partenaire conclut que les Données à caractère personnel du Partenaire transférées ne bénéficient pas de garanties appropriées, il peut résilier immédiatement le Contrat applicable conformément à la clause de résiliation pour convenance dudit Contrat ou, en l'absence d'une telle provision, en en informant Google.

2.5 *Aucune intention de modification des CCT turques*. Rien dans le Contrat (y compris le présent Avenant) n'a pour intention de modifier ou de contredire les CCT turques ni de porter préjudice aux libertés et droits fondamentaux des personnes concernées accordés par la Législation turque sur la protection des données.

2.6 *Priorité des CCT*. En cas de conflit ou d'incohérence entre les CCT turques (qui sont intégrées par référence dans les présentes dès lors que le Partenaire les a signées) et le reste du Contrat (y compris le présent Avenant), les CCT turques prévalent.

Israël

1. Définition supplémentaire.

- « *Loi israélienne sur la protection de la confidentialité* » désigne la loi israélienne de 1981 sur la protection de la confidentialité et toutes les réglementations qui en découlent.

2. Termes équivalents. Tout terme équivalant à « responsable du traitement », « données à caractère personnel », « traitement » et « sous-traitant » utilisé dans les présentes à la signification qui lui est attribuée dans la Loi israélienne sur la protection de la confidentialité.

3. Droits d'audit du Partenaire. Google s'engage à permettre au Partenaire ou à un auditeur indépendant désigné par celui-ci d'effectuer des audits (y compris des inspections), comme décrit à la Section 7.5.2(a) (Audit par le Partenaire).

Annexe 4 : Produits spécifiques

Les conditions décrites dans chaque sous-section de la présente Annexe 4 ne s'appliquent qu'à l'égard du traitement des Données du Partenaire par le(s) Service(s) correspondant(s).

Google Cloud Platform

1. Définitions supplémentaires.

- « *Compte* », s'il n'est pas défini dans le Contrat, désigne le compte Google Cloud Platform du Partenaire.
- « *Google Cloud Platform* » désigne les services Google Cloud Platform décrits sur la page https://cloud.google.com/terms/services, à l'exclusion des éventuelles Offres tierces.
- « *Offres tierces* », s'il n'est pas défini dans le Contrat, désigne (a) les services, logiciels, produits et autres offres de tiers qui ne sont pas intégrés dans Google Cloud Platform ou dans le Logiciel, (b) les offres identifiées à la section « Conditions tierces » des Conditions spécifiques des Services du Contrat, et (c) les systèmes d'exploitation tiers.

2. Certifications de conformité. Les Certifications de conformité pour les Services audités de Google Cloud Platform incluent également les certificats pour ISO 27017 et ISO 27018 ainsi qu'une Attestation de conformité PCI DSS.

3. Emplacements des centres de données. Les emplacements des centres de données de Google Cloud Platform sont décrits sur la page https://cloud.google.com/about/locations/.

4. Informations sur les Sous-traitants indirects. Les noms, emplacements et activités des Sous-traitants indirects de Google Cloud Platform sont décrits sur la page https://cloud.google.com/terms/subprocessors.

5. Équipe chargée de la protection des données dans le cloud. L'Équipe chargée de la protection des données pour Google Cloud Platform peut être contactée à l'adresse https://support.google.com/cloud/contact/dpo.

6. Informations sur les Transferts limités. Des informations supplémentaires pertinentes concernant les Transferts limités, Contrôles de sécurité supplémentaires et autres mesures de protection complémentaires sont disponibles sur la page https://cloud.google.com/privacy.

7. Conditions spécifiques des Services.

Solution Bare Metal (Google Cloud Platform)

La solution Bare Metal fournit un accès non virtualisé aux ressources d'infrastructure sous-jacentes et a été conçu avec certaines caractéristiques distinctes.

1. Modifications. Le présent Avenant est modifié comme suit en ce qui concerne la solution Bare Metal :

- La définition d'« Auditeur tiers de Google » est remplacée par la suivante :
    - « *Auditeur tiers de Google* » fait référence à un auditeur tiers qualifié et indépendant désigné par Google ou par un Sous-traitant indirect de la solution Bare Metal et dont Google s'engage à divulguer l'identité au Partenaire à la demande de celui-ci.

- Les formulations suivantes ont été supprimées :
    - Dans la Section 7.1.1 (Mesures de sécurité de Google), la formulation « pour permettre le chiffrement des Données du Partenaire ».
    - Dans l'Annexe 2 (Mesures de sécurité), les sous-sections de la Section 1(a) intitulées « Systèmes d'exploitation serveur » et « Continuité des activités »).
    - Dans l'Annexe 2, les sous-sections de la Section 1(b) intitulées « Surface d'attaque externe », « Détection des intrusions » et « Technologies de chiffrement ».
    - Dans l'Annexe 2, les phrases suivantes de la Section 3(a) :
        - Google stocke les données dans un environnement mutualisé, sur des serveurs qui lui appartiennent. Sauf instructions contraires (comme la sélection d'un emplacement pour les données, par exemple), Google réplique les données du Partenaire sur plusieurs centres de données dispersés géographiquement.

2. Certifications de conformité et Rapports SOC. Google ou son Sous-traitant indirect s'engagent à maintenir au minimum les évaluations vis-à-vis des normes suivantes (ou une alternative équivalente ou de niveau supérieur) pour la solution Bare Metal afin de vérifier l'efficacité continue des Mesures de sécurité :

a. un certificat pour ISO 27001 et une Attestation de conformité PCI DSS (les « *Certifications de conformité BMS* ») ; et

b. des rapports SOC 1 et SOC 2 mis à jour tous les ans sur la base d'un audit réalisé au moins tous les 12 mois (les « *Rapports SOC BMS* »).

3. Examen de la Documentation sur la sécurité. Pour démontrer qu'il se conforme à ses obligations au titre du présent Avenant, Google s'engage à mettre à la disposition du Partenaire les Certifications de conformité BMS et les Rapports SOC BMS pour que le Partenaire puisse les examiner et, si le Partenaire est un sous-traitant, s'engage à permettre au Partenaire de demander accès aux Rapports SOC BMS pour le responsable du traitement concerné conformément à la Section 7.5.3 (Conditions supplémentaires pour les examens et les audits).

4. Obligations du Partenaire. Sans limiter les obligations expresses de Google en lien avec la solution Bare Metal, le Partenaire s'engage à prendre des mesures raisonnables afin de protéger les Données du Partenaire et autres contenus stockés ou traités sur la solution Bare Metal et d'en préserver la sécurité.

5. Clause de non-responsabilité. Nonobstant toute disposition contraire dans le Contrat (y compris le présent Avenant), Google ne peut être tenu responsable, en ce qui concerne la solution Bare Metal, de :

a. la sécurité non physique, comme les contrôles des accès, le chiffrement, les pare-feu, la protection antivirus, la détection des menaces et les analyses de sécurité ;

b. la journalisation et la surveillance ;

c. la maintenance et l'assistance autres que matérielles ;

d. la sauvegarde des données, y compris pour toute redondance ou configuration de haute disponibilité ; ou

e. toute politique ou procédure de continuité de l'activité ou de reprise après sinistre.

Le Partenaire est seul responsable de la sécurité (autre que la sécurité physique des serveurs de la solution Bare Metal), la journalisation et la surveillance, la maintenance et l'assistance, ainsi que la sauvegarde des Systèmes d'exploitation, Données du Partenaire, logiciels et applications que le Partenaire utilise, importe ou héberge sur la solution Bare Metal.

Cloud NGFW (Google Cloud Platform)

L'édition de Cloud NGFW intitulée « Cloud NGFW Enterprise » (« CNE ») est conçue pour atténuer les risques liés à la cybersécurité et présente de ce fait certaines caractéristiques distinctes.

1. Modifications. L'Avenant est modifié comme suit en ce qui concerne CNE :

- Les Sections 6.1 (Suppression par le Partenaire) et 6.2 (Restitution ou suppression à l'expiration de la Période de validité) n'empêchent pas Google ni les Sous-traitants indirects de conserver un fichier ou une capture de paquet de trafic réseau qui a été soumis(e) à des fins de TTS et désigné(e) par CNE comme une menace de sécurité, à condition toutefois que le fichier ou la capture de paquet de trafic réseau n'inclue pas de Données à caractère personnel du Partenaire.

Google Distributed Cloud Edge (Google Cloud Platform)

Google Distributed Cloud Edge (« *GDCE* ») n'est pas déployé dans un centre de données Google. Il a été conçu avec certaines caractéristiques distinctes.

1. Modifications. Le présent Avenant est modifié comme suit en ce qui concerne GDCE :

- Les références aux « systèmes Google » sont remplacées par « l'Équipement ».
- La Section 6.2 (Restitution ou suppression à l'expiration de la Période de validité) est remplacée comme suit :
    - 6.2 *Restitution ou suppression à l'expiration de la Période de validité*. Le Partenaire demande à Google de supprimer toutes les Données restantes du Partenaire (y compris les copies existantes) de l'Équipement à la fin de la Période de validité, conformément au droit applicable. Si le Partenaire souhaite conserver des Données du Partenaire après l'expiration de la Période de validité, il peut exporter lesdites données ou en effectuer des copies avant l'expiration de la Période de validité. Google s'engage à se conformer à l'Instruction formulée dans la présente Section 6.2 dans les meilleurs délais pratiques et raisonnables et sous 180 jours au maximum, à moins que la Législation européenne (lorsque la Législation européenne sur la protection des

données s'applique) ou la législation pertinente (lorsque tout autre Droit applicable relatif à la confidentialité s'applique) ne requière le stockage desdites données.

- Les mots suivants sont ajoutés à la fin de la Section 10.1 (Installations de stockage et de traitement des données) : « ou quel que soit le pays où se trouvent les installations du Client ».

- La Section 1 (Centre de données et sécurité réseau) de l'Annexe 2 (Mesures de sécurité) est remplacée par ce qui suit :

    - **1. Machines locales et sécurité réseau**

      Machines locales. Les Données du Partenaire ne sont stockées que sur l'Équipement devant être déployé sur le site d'implantation du client.

      Systèmes d'exploitation serveur. Les serveurs Google utilisent une implémentation Linux personnalisée pour l'environnement d'application. Google applique un processus de revue de code afin d'accroître la sécurité du code utilisé pour fournir GDCE et d'améliorer les produits de sécurité dans les environnements de production GDCE.

      Technologies de chiffrement. Google propose le chiffrement HTTPS (également appelé connexion SSL ou TLS) et autorise le chiffrement des données en transit. Les serveurs Google acceptent 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) contribuent à protéger le trafic et à minimiser l'impact d'une clé compromise ou d'une avancée en matière de cryptographie. Google offre également un chiffrement des données au repos avec au minimum l'utilisation d'AES128 ou d'un algorithme équivalent. GDCE bénéficie d'une intégration CMEK. Des informations complémentaires sont accessibles sur la page https://cloud.google.com/kms/docs/cmek.

      Connexion à Cloud VPN. Google autorise le Partenaire à activer et configurer une interconnexion chiffrée solide entre l'Équipement et le cloud privé virtuel du Partenaire à l'aide de Cloud VPN et via une connexion VPN IPsec.

      Stockage lié. Le stockage des données du Partenaire est lié au serveur. En cas de vol ou de copie d'un disque au repos, le contenu dudit disque est irrécupérable en dehors du serveur.

- La Section 2 (Contrôles des accès et sites) et la Section 3 (Données) de l'Annexe 2 (Mesures de sécurité) sont supprimées.

2. Clauses non applicables. Toute obligation de Google stipulée dans le Contrat (y compris le présent Avenant) ou dans la documentation sur la sécurité associée (y compris les livres blancs) qui dépend de l'exploitation d'un centre de données Google par Google ne s'applique pas à GDCE.

Multicloud géré par Google (Google Cloud Platform)

Les Services multicloud (MCS) gérés par Google nécessitent des infrastructures tierces et ont été conçus avec certaines caractéristiques distinctes.

1. Définition supplémentaire.

- « *Avenant relatif au traitement des données pour les MCS gérés par Google* » désigne les conditions publiées sur la page https://cloud.google.com/terms/mcs-data-processing-terms.

2. Conditions relatives au traitement des données sur le multicloud. L'Avenant relatif au traitement des données pour les MCS gérés par Google complète et modifie les présentes en ce qui concerne les Services multicloud gérés par Google pour Google Cloud Platform.

Google Cloud VMware Engine (Google Cloud Platform)

Il est possible que Google n'ait pas accès à l'environnement VMware du Partenaire ou ne puisse chiffrer les données à caractère personnel dans l'environnement VMware du Partenaire.

NetApp Volumes (Google Cloud Platform)

1. Modifications. Le présent Avenant est modifié comme suit en ce qui concerne NetApp Volumes :

- La définition d'« Auditeur tiers de Google » est remplacée par la suivante :
    - « *Auditeur tiers de Google* » fait référence à un auditeur tiers qualifié et indépendant désigné par Google ou par un Sous-traitant indirect de NetApp Volumes et dont Google s'engage à divulguer l'identité au Partenaire à la demande de celui-ci.
- La Section 3(a) (Stockage des données, isolation et journalisation) de l'Annexe 2 (Mesures de sécurité) est remplacée par ce qui suit :
    - (a) *Stockage, isolation et journalisation des données*. Google stocke les données dans un environnement à plusieurs locataires sur des serveurs détenus par NetApp, Inc. Sauf Instructions contraires (sélection d'un emplacement pour les données, par exemple), Google réplique les données du Partenaire sur plusieurs centres de données dispersés géographiquement. Google applique également une isolation logique pour les Données du Partenaire. Le Partenaire se voit confier le contrôle de certaines règles de partage des données. Lesdites règles, conformément aux fonctionnalités des Services, permettent au Partenaire de déterminer les paramètres de partage de produit qui s'appliquent aux Utilisateurs finaux du Partenaire pour des besoins particuliers. Le Partenaire peut choisir d'utiliser la fonctionnalité de journalisation fournie par Google via les Services.

2. Certifications de conformité et Rapports SOC. Google ou son Sous-traitant indirect s'engagent à obtenir au minimum les certifications et rapports suivants (ou une alternative équivalente ou de niveau supérieur) pour NetApp Volumes :

a. un certificat pour ISO 27001 et une Attestation de conformité PCI DSS (les « *Certifications de conformité NetApp* ») ; et

b. des rapports SOC 1 et SOC 2 mis à jour tous les ans sur la base d'un audit réalisé au moins tous les 12 mois (les « *Rapports SOC NetApp* »).

3. Examen de la Documentation sur la sécurité. Pour démontrer qu'il se conforme à ses obligations en vertu du présent Avenant, Google s'engage à mettre à la disposition du Partenaire les Certifications de conformité NetApp et les Rapports SOC NetApp pour que le Partenaire puisse les examiner et, si le Partenaire est un sous-traitant, s'engage à permettre au Partenaire de demander l'accès aux Rapports SOC NetApp pour le responsable du traitement concerné conformément à la Section 7.5.3 (Conditions supplémentaires pour les examens et les audits).

Looker (original)

1. Définitions supplémentaires.

- « *Console d'administration* » désigne toute console d'administration applicable à chaque instance.
- « *Avenant relatif au traitement des données pour les MCS gérés par Google* » désigne, le cas échéant, les conditions publiées sur la page https://cloud.google.com/terms/mcs-data-processing-terms.
- « *Services multicloud gérés par Google* » désigne, le cas échéant, les services, produits et fonctionnalités Google spécifiés qui sont hébergés sur l'infrastructure d'un fournisseur de services cloud tiers.
- « *Looker (original)* » désigne une plate-forme intégrée (y compris l'infrastructure dans le cloud, le cas échéant, et les composants logiciels, y compris les API associées) qui permet aux entreprises d'analyser des données et de définir des métriques métier pour plusieurs sources de données qui ont été fournies au Partenaire par Google en vertu du Contrat. Looker (original) exclut les Offres tierces.
- « *Fournisseur tiers* de *services multicloud* » a la signification qui lui est attribuée dans l'Avenant relatif au traitement des données pour les MCS gérés par Google.
- « *Formulaire de commande* » a la signification qui lui est attribuée dans le Contrat, sauf si le Partenaire a effectué l'achat via un revendeur ou une place de marché en ligne ou qu'il utilise Looker uniquement dans le cadre d'un essai ou à des fins d'évaluation au titre d'un contrat, auquel cas le Formulaire de commande peut désigner un autre formulaire écrit (y compris un formulaire transmis par courriel ou par un autre moyen électronique) tel qu'autorisé par Google.

2. Modifications. Le présent Avenant est modifié comme suit en ce qui concerne Looker (original) :

- La définition du terme « Adresse courriel de notification » est remplacée par la suivante :

- « *Adresse courriel de notification* » fait référence à la ou aux adresses courriel désignées par le Partenaire dans le Formulaire de commande ou via Looker (selon le cas) pour recevoir certaines notifications de la part de Google.

- Les définitions de « CCT (responsable du traitement à sous-traitant) », « CCT (sous-traitant à responsable du traitement) », « CCT (sous-traitant à sous-traitant) » et « CCT (sous-traitant à sous-traitant, exportateur Google) » dans l'Annexe 3 (Droits spécifiques relatifs à la confidentialité) sont remplacées par les suivantes :

  - « *CCT (responsable du traitement à sous-traitant)* » désigne les conditions publiées sur la page https://cloud.google.com/terms/looker/legal/sccs/eu-c2p

  - « *CCT (sous-traitant à responsable du traitement)* » désigne les conditions publiées sur la page https://cloud.google.com/terms/looker/legal/sccs/eu-p2c

  - « *CCT (sous-traitant à sous-traitant)* » désigne les conditions publiées sur la page https://cloud.google.com/terms/looker/legal/sccs/eu-p2p

  - « *CCT (sous-traitant à sous-traitant, exportateur Google)* » désigne les conditions publiées sur la page https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group

- Les mots suivant sont ajoutés à la fin de la Section 10.1 (Installations de stockage et traitement des données) : « ou quel que soit le pays où les fournisseurs tiers de services multicloud disposent d'installations. »

3. Responsabilités supplémentaires du Partenaire en matière de sécurité. Le Partenaire est responsable de la sécurité de son environnement, de ses bases de données et de ses configurations pour Looker (original), à l'exception des systèmes gérés et contrôlés par Google.

4. Certifications de conformité et Rapports SOC. Les Certifications de conformité et les Rapports SOC pour les Services audités de Looker (original) peuvent varier selon l'environnement d'hébergement où sont utilisés les Services concernés. Google s'engage à fournir sur demande des informations détaillées sur les Certifications de conformité et les Rapports SOC disponibles pour des environnements d'hébergement spécifiques.

5. Emplacements des centres de données. Les emplacements des centres de données de Looker (original) sont décrits dans le Formulaire de commande applicable ou autrement identifiés par Google.

6. Aucune obligation de certification par les Partenaires basés hors de la région EMEA. Le Partenaire n'est pas tenu d'attester de son Autorité de contrôle compétente ou de l'identifier tel que décrit à la Section 4.2 (Certification par les Partenaires basés hors de la région EMEA) des conditions relatives à la protection des données en Europe dans l'Annexe 3 (Droits spécifiques relatifs à la confidentialité) pour Looker (original).

7. Informations sur les Transferts limités. Des informations supplémentaires pertinentes concernant les Transferts limités, Contrôles de sécurité supplémentaires et autres mesures de protection complémentaires pour Looker (original) sont disponibles sur la page https://docs.looker.com.

8. Informations sur les Sous-traitants indirects. Les noms, emplacements et activités des Sous-traitants indirects pour Looker (original) sont décrits sur les pages suivantes :

a. https://cloud.google.com/terms/looker/privacy/lookeroriginal-subprocessors ; et

b. https://cloud.google.com/terms/subprocessors.

9. Multicloud géré par Google (Looker (original))

Les Services multicloud (MCS) gérés par Google nécessitent des infrastructures tierces et ont été conçus avec certaines caractéristiques distinctes.

9.1 *Conditions relatives au traitement des données dans les environnements multicloud*. L'Avenant relatif au traitement des données pour les MCS gérés par Google complète et modifie les présentes en ce qui concerne les Services multicloud gérés par Google pour Looker (original).

10. Équipe chargée de la protection des données dans le cloud. L'Équipe chargée de la protection des données pour Looker (original) peut être contactée à l'adresse https://support.google.com/cloud/contact/dpo.

11. Archives de traitement de Google. Dans la mesure où le Droit applicable relatif à la confidentialité exige de Google qu'il collecte et conserve certaines informations concernant le Partenaire ou ses Clients, le Partenaire s'engage à fournir lesdites informations à Google sur demande et à informer Google de toute mise à jour éventuelle requise pour les garder exactes et à jour, sauf si Google demande au Partenaire de fournir et mettre à jour lesdites informations par d'autres moyens.

12. Mesures de sécurité supplémentaires pour les applications. Google s'engage à mettre en œuvre et à garder opérationnelles les Mesures de sécurité supplémentaires décrites ci-dessous pour Looker (original) :

a. Google suit au minimum les pratiques standards dans l'industrie en ce qui concerne l'architecture de sécurité. Les serveurs proxy utilisés avec les applications Google aident à sécuriser l'accès à Looker en fournissant un point unique de filtrage des attaques via une liste de blocage IP et une limitation du débit de connexion.

b. Les administrateurs du Partenaire contrôlent les accès aux applications par le personnel de Google fournissant l'assistance technique requise par le Partenaire ou par les Utilisateurs finaux du Partenaire.

Services SecOps

1. Définitions supplémentaires.

- « *Compte* », s'il n'est pas défini dans le Contrat, désigne le compte des Services SecOps du Partenaire ou le compte Google Cloud Platform, selon le cas.

- « *Services SecOps* » désigne les solutions Chronicle SIEM, Chronicle SOAR et Mandiant, telles que décrites sur la page https://cloud.google.com/terms/secops/services, à l'exclusion des Offres tierces. Par souci de clarification, les Services SecOps excluent les Services Mandiant Consulting et les Services gérés Mandiant.

- « *Offres tierces* », si le terme n'est pas défini dans le Contrat, désigne (a) les services, logiciels, produits et autres offres de tiers qui ne sont pas intégrés aux Services SecOps ou au Logiciel et (b) les systèmes d'exploitation tiers.

2. Modifications. Le présent Avenant est modifié comme suit en ce qui concerne les Services SecOps :

- La définition de « Contrôles de sécurité supplémentaires » est remplacée par la suivante :

    - *« Contrôles de sécurité supplémentaires »* désigne les ressources, fonctions, fonctionnalités et/ou contrôles de sécurité (le cas échéant) que le Partenaire peut utiliser à sa discrétion et/ou comme il le juge approprié, y compris, le cas échéant, le chiffrement, la journalisation et la surveillance, la gestion de l'authentification et des accès et l'analyse de sécurité.

- La définition de « Services audités » est remplacée par la suivante :

    - « *Services audités* » désigne les Services SecOps alors en vigueur décrits comme entrant dans le champ d'application de la certification ou du rapport concerné, présentés sur la page https://cloud.google.com/security/compliance/secops/services-in-scope. Google ne peut effacer des Services SecOps de cette URL que s'ils ont été arrêtés conformément au Contrat.

- Les définitions de « CCT (responsable du traitement à sous-traitant) », « CCT (sous-traitant à responsable du traitement) », « CCT (sous-traitant à sous-traitant) » et « CCT (sous-traitant à sous-traitant, exportateur Google) » dans l'Annexe 3 (Droits spécifiques relatifs à la confidentialité) sont remplacées par les suivantes :

    - « *CCT (responsable du traitement à sous-traitant)* » désigne les conditions publiées sur la page https://cloud.google.com/terms/secops/sccs/eu-c2p

    - « *CCT (sous-traitant à responsable du traitement)* » désigne les conditions publiées sur la page https://cloud.google.com/terms/secops/sccs/eu-p2c.

    - « *CCT (sous-traitant à sous-traitant)* » désigne les conditions publiées sur la page https://cloud.google.com/terms/secops/sccs/eu-p2p

    - « *CCT (sous-traitant à sous-traitant, exportateur Google)* » désigne les conditions publiées sur la page https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter

- La Section 7.4 (Certifications de conformité et Rapports SOC) de l'Avenant est modifiée comme suit :

    - 7.4 *Certifications de conformité et Rapports SOC*. Google s'engage à maintenir au minimum les certifications et rapports identifiés sur la page https://cloud.google.com/security/compliance/secops/services-in-scope pour les Services audités afin de vérifier l'efficacité continue des Mesures de sécurité (les « Certifications de conformité » et « Rapports SOC »).

      Google peut ajouter des normes à tout moment. Google se réserve le droit de trouver une alternative équivalente ou de niveau supérieur à une Certification de conformité ou à un Rapport SOC.

3. Emplacements des centres de données. Les emplacements des centres de données des Services SecOps sont décrits sur la page https://cloud.google.com/terms/secops/data-residency.

4. Aucune obligation de certification par les Partenaires basés hors de la région EMEA. Le Partenaire n'est pas tenu d'attester de son Autorité de contrôle compétente ou de l'identifier tel que décrit à la Section 4.2 (Certification par les Partenaires basés hors de la région EMEA) des conditions relatives à la protection des données en Europe dans l'Annexe 3 (Droits spécifiques relatifs à la confidentialité) pour les Services SecOps.

5. Informations sur les Sous-traitants indirects. Les noms, emplacements et activités des Sous-traitants indirects pour les Services SecOps sont décrits sur la page https://cloud.google.com/terms/secops/subprocessors.

6. Équipe chargée de la protection des données dans le cloud. L'Équipe chargée de la protection des données pour les Services SecOps peut être contactée à l'adresse https://support.google.com/cloud/contact/dpo (et/ou par tout autre moyen que peut proposer Google à certaines occasions).

7. Archives de traitement de Google. Dans la mesure où le Droit applicable relatif à la confidentialité exige de Google qu'il collecte et conserve certaines informations concernant le Partenaire, le Partenaire s'engage à fournir lesdites informations à Google sur demande et à informer Google de toute mise à jour éventuelle requise pour les garder exactes et à jour, sauf si Google demande au Partenaire de fournir et mettre à jour lesdites informations par d'autres moyens.

Précédentes versions des Conditions relatives à la sécurité et au traitement des données (Partenaires) :

30 juin 2022 24 septembre 2021 20 août 2020 10 août 2020 17 juillet 2020 1er octobre 2019 28 février 2019 25 mai 2018 13 mars 2018

Précédentes versions des Conditions relatives à la sécurité et au traitement des données pour les Services SecOps (Partenaires) :

6 février 2023 31 octobre 2022 27 septembre 2021

Versions précédentes *(dernière modification : 30 octobre 2024)*

15 octobre 2024 26 septembre 2024 9 septembre 2024 9 avril 2024 8 novembre 2023 15 août 2023 20 septembre 2022