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

Le présent Avenant relatif au traitement des données dans le cloud (y compris ses annexes, l'« *Avenant* ») est intégré au(x) Contrat(s) (tel que défini ci-dessous) conclu(s) entre Google et le Client. Cet Avenant était auparavant appelé « Conditions relatives à la sécurité et au traitement des données » dans le cadre d'un contrat pour Google Cloud Platform, Looker (original), les Services Google SecOps ou Google Cloud Skills Boost pour les Entreprises ; « Avenant relatif au traitement des données » pour les contrats Google Workspace ou Cloud Identity et « Avenant relatif au traitement des données » pour les contrats de Services Mandiant Consulting et de Services gérés Mandiant.

Conditions générales

1. Présentation

Le présent Avenant décrit les obligations des parties, y compris en vertu des lois applicables concernant la confidentialité, la sécurité et la protection des données, pour ce qui a trait au traitement et à la sécurité des Données du Client (telles que définies ci-dessous). Cet Avenant prendra effet à la Date d'entrée en vigueur de l'Avenant (telle que définie ci-dessous) et remplacera les éventuelles conditions auparavant applicables au traitement et à la sécurité des Données du Client. 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 Client a accepté le présent Avenant ou 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 Client 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 Client.
- « *Droit applicable relatif à la confidentialité* » correspond, dans le cadre du traitement des Données à caractère personnel du Client, à toute loi ou réglementation provinciale, d'un État

américain, de l'Union européenne, fédérale, nationale ou autre relative à 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 pertinent disponible à l'adresse https://cloud.google.com/security/compliance/services-in-scope. Google ne peut effacer de Services de cette URL que s'ils ont été arrêtés conformément au Contrat applicable.

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

- « *Données du Client* », si le terme n'est pas défini dans le Contrat, a la signification qui lui est attribuée à l'Annexe 4 (Produits spécifiques).

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

- « *Incident lié aux données* » désigne une violation de la sécurité de Google qui entraîne, de manière accidentelle ou illégale, la destruction, la perte, l'altération ou encore la divulgation non autorisée des Données du Client sur des systèmes gérés ou contrôlés par Google, ou encore l'accès non autorisé à ces 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 contexte : (a) le RGPD ou (b) la Loi fédérale sur la protection des données (LPD) de la Suisse.

- « *Législation européenne* » désigne, selon le contexte : (a) la législation de l'UE ou d'un État membre de l'UE (si le RGPD de l'UE s'applique au traitement des Données à caractère personnel du Client) ; (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 Client) ; ou (c) la législation de la Suisse (si la LPD suisse s'applique au traitement des Données à caractère personnel du Client).

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

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

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

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

- « *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 à 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 en vertu du présent Avenant pour traiter les Données du Client en vue de fournir certains Services et SAT (Services d'assistance technique), le cas échéant.

- « *Autorité de contrôle* » désigne, selon le contexte : (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 contexte, 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 nouvelle Loi fédérale 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 qu'amendé et incorporé dans la législation du Royaume-Uni en application de la loi sur le retrait de l'Union européenne (European Union Withdrawal Act) de 2018, ainsi que toutes les lois secondaires applicables conformément à cette 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, tels que requis par le Droit applicable relatif à la confidentialité.

3. Durée

Quand bien même le Contrat applicable serait résilié ou arrivé à expiration, le présent Avenant demeure en vigueur jusqu'à ce que Google supprime toutes les Données du Client tel que décrit dans cet Avenant, et expire automatiquement au même moment.

4. Rôles ; Conformité légale

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

4.2 *Résumé du traitement*. L'objet et les détails du traitement des Données à caractère personnel du Client sont décrits 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 Client en vertu du Droit applicable relatif à la confidentialité.

4.4 *Conditions légales supplémentaires*. Lorsque le traitement des Données à caractère personnel du Client 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 tel que décrit à la Section 14.1 (Priorité).

5. Traitement de données

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

a. Le Client offre une garantie continue que le responsable du traitement pertinent a autorisé :

i. les Instructions ;

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

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

b. Le Client s'engage à transmettre sans délai ni retard injustifié au responsable du traitement concerné tout avis émis par Google au titre des Sections 7.2.1 (Notification d'incident), 9.2.1 (Responsabilité des demandes) ou 11.4 (Possibilité de s'opposer à des Sous-traitants indirects) ;

c. Le Client peut mettre à disposition du responsable du traitement concerné toute autre information mise à disposition par Google au titre du présent Avenant concernant l'emplacement des Centres de données Google ou les noms, emplacements et activités des Sous-traitants indirects.

5.2 *Conformité avec les Instructions du Client*. Le Client demande à Google de traiter les Données du Client conformément au Contrat applicable (et au présent Avenant) uniquement comme suit :

a. pour fournir, sécuriser et surveiller les Services et SAT (le cas échéant) ; et

b. tel que spécifié :

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

ii. dans toute autre instruction écrite fournie par le Client et acceptée par Google comme instruction aux fins 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 pertinente (lorsque tout autre Droit applicable relatif à la confidentialité s'applique) ne l'en empêche.

6. Suppression des données

6.1 *Suppression par le Client*. Google permet au Client de supprimer les Données client au cours de la Période de validité et d'une manière conforme aux fonctionnalités des Services. Si le Client utilise les Services pour supprimer des Données du Client au cours de la Période de validité et que ces Données du Client ne peuvent pas être récupérées par le Client, cette utilisation constituera une Instruction donnée à Google de supprimer les Données du Client concernées des systèmes de Google. Google s'engage à respecter cette Instruction 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 de ces données.

6.2 *Restitution ou suppression à l'expiration de la Période de validité*. Si le Client souhaite conserver certaines Données du Client après la Période de validité, il peut demander à Google, conformément à la Section 9.1 (Accès ; Rectification ; Traitement restreint ; Portabilité) de lui restituer lesdites données pendant la Période de validité. Sous réserve de la Section 6.3 (Instruction de suppression différée), le Client demande à Google de supprimer toutes les Données du Client restantes (y compris toute copie existante) des systèmes de Google à l'expiration de la Période de validité. À l'issue d'une période de récupération allant jusqu'à 30 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 pertinente (lorsque tout autre Droit applicable relatif à la confidentialité s'applique) ne requière le stockage desdites données.

6.3. *Instruction de suppression différée*. Dans la mesure où des Données du Client couvertes par l'Instruction de suppression décrite à la Section 6.2 (Restitution ou suppression à l'expiration de la Période de validité) sont également traitées, à l'expiration de la Période de validité définie à la Section 6.2, en relation avec un Contrat avec une Période de validité étendue, une telle instruction de suppression prendra effet pour lesdites Données du Client uniquement lorsque la Période de validité étendue aura expiré. En d'autres termes, le présent Avenant continuera de s'appliquer à ces Données du Client jusqu'à leur suppression par Google.

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 à garantir des mesures techniques, organisationnelles et physiques pour protéger les Données du Client contre les destructions, pertes, altérations, ou divulgations ou accès non autorisés, de manière accidentelle ou illégale, 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 Client ; pour garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services de Google ; pour rétablir rapidement l'accès aux Données du Client à la suite d'un incident ; et pour tester régulièrement leur efficacité. Google est susceptible de mettre à jour les Mesures de sécurité de temps en temps 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, contractants et Sous-traitants indirects à accéder aux Données du Client que dans la mesure strictement nécessaire pour se conformer aux Instructions ;

b. prendre des mesures raisonnables pour s'assurer que ses employés, contractants 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 Client se sont engagées à respecter leur caractère confidentiel.

7.1.3 *Contrôles de sécurité supplémentaires*. Google rendra des Contrôles de sécurité supplémentaires disponibles dans le but de :

a. permettre au Client de prendre des mesures pour sécuriser ses Données ; et

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

7.1.4 *Assistance de Google en matière de sécurité*. Selon la nature du traitement des Données à caractère personnel du Client et selon les informations à sa disposition, Google s'engage à aider le Client à s'assurer qu'il respecte ses obligations (ou les obligations du responsable du traitement concerné si le Client 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 garantissant 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 applicable (y compris le présent Avenant) ; et

e. si les sous-sections (a) à (d) ci-dessus ne suffisent pas à permettre au Client (ou au responsable du traitement concerné) de respecter lesdites obligations, en offrant au Client 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 le Client d'un Incident lié aux données dès qu'il en a connaissance, sans délai ni retard injustifié, et de prendre rapidement des mesures raisonnables afin de minimiser les dommages et de sécuriser les Données du Client.

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 Client qui sont touchées ; les mesures que Google a prises ou compte prendre pour remédier à l'Incident lié aux données et mitiger les risques éventuels ; les éventuelles mesures que Google recommande au Client 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 dès qu'elles deviennent disponibles.

7.2.3 *Absence d'évaluation des Données du Client par Google*. Google n'est pas tenu d'évaluer les Données du Client en vue d'identifier 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 Client en matière de sécurité et évaluation de la sécurité*.

7.3.1 *Responsabilités du Client en matière de sécurité*. Sans préjudice des obligations de Google décrites dans les Sections 7.1 (Mesures et contrôles de sécurité, et assistance de Google en matière de sécurité) et 7.2 (Incidents liés aux données), et dans toute autre partie du Contrat applicable, le Client est tenu pour responsable de son utilisation des Services et du stockage de toute copie des Données du Client en dehors des systèmes de Google ou 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 Client ;

b. la sécurisation des identifiants d'authentification du compte, des systèmes et appareils qu'utilise le Client pour accéder aux Services, et ;

c. la sauvegarde ou la conservation de copies des Données du Client, selon le cas.

7.3.2 *Évaluation de la sécurité par le Client*. Le Client accepte que les Services, Mesures de sécurité, Contrôles de sécurité supplémentaires, et les engagements de Google en vertu de cette Section 7 (Sécurité des données) offrent un niveau de sécurité adapté au risque auquel sont exposées les Données du Client (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 Client ainsi que des risques pour les personnes physiques).

7.4 *Certifications de conformité et Rapports SOC*. Google s'engage à maintenir au minimum les normes suivantes pour les Services audités afin de vérifier l'efficacité continue des Mesures de sécurité :

a. des certificats pour ISO 27001 et toutes autres certifications supplémentaires décrites dans l'Annexe 4 (Produits spécifiques) (les « *Certifications de conformité* ») ; et

b. des rapports SOC 2 et SOC 3 produits par l'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 se réserve le droit d'ajouter des normes à tout moment. Google se réserve le droit de trouver une alternative équivalente ou améliorée à une Certification de conformité ou à un Rapport SOC.

7.5 *Examens et audits de conformité*.

7.5.1 *Examen de la Documentation relative à 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 Client la Documentation relative la sécurité en vue de son examen et, si le Client est un sous-traitant, s'engage à permettre au Client de demander accès aux Rapports SOC pour le 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 Client*.

a. *Audit par le Client*. Si le Droit applicable relatif à la confidentialité l'exige, Google s'engage à autoriser le Client ou un auditeur indépendant désigné par le Client 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). Pendant un audit, Google s'engage à faire preuve d'une coopération raisonnable avec le Client ou son auditeur tel que décrit dans la Section 7.5 (Examens et audits de conformité).

b. *Examen indépendant par le Client*. Le Client peut aussi effectuer un audit pour vérifier que Google respecte ses obligations en vertu du présent Avenant en examinant la Documentation relative à la sécurité (qui reflète les résultats des audits réalisés par l'Auditeur tiers de Google).

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

a. Le Client 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 relative à la sécurité) ; ou

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

b. Suite à une demande du Client en vertu de la Section 7.5.3(a), Google et le Client conviendront à l'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 relative à 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 Client), ainsi que des contrôles de confidentialité et de sécurité qui s'y appliquent.

c. Google se réserve le droit de facturer des frais (basés sur les coûts raisonnables de Google) pour tout audit en vertu de la Section 7.5.2(a) (Audit par le Client). Google fournira au Client des informations supplémentaires concernant les frais applicables et la base de leur calcul avant tout audit. Le Client est responsable des frais facturés par l'auditeur qu'il a nommé pour effectuer l'audit.

d. Google peut s'opposer par écrit au fait qu'un auditeur désigné par le Client effectue un audit conformément à la Section 7.5.2(a) (Audit par le Client) si l'auditeur, de l'avis raisonnable de Google, n'est pas suffisamment compétent ou indépendant, est un concurrent de Google ou est manifestement inadapté. Dans le cas d'une telle objection par Google, le Client doit nommer 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 Client 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 Client à s'assurer qu'il respecte ses obligations (ou les obligations du responsable du traitement concerné si le Client 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 relative à la sécurité conformément à la Section 7.5.1 (Examen de la Documentation relative à la sécurité) ;

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

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

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

9.1 *Accès ; Rectification ; Traitement restreint ; Portabilité*. Au cours de la Période de validité, Google, tout en respectant les fonctionnalités des Services, s'engage à permettre au Client d'accéder aux Données du Client, de les rectifier et d'en restreindre le traitement, y compris via la fonctionnalité de suppression fournie par Google telle que décrite dans la Section 6.1 (Suppression par le Client), et d'exporter les Données du Client. Si le Client découvre que des Données à caractère personnel du Client sont inexactes ou obsolètes, il s'engage à être responsable de l'utilisation desdites fonctionnalités pour rectifier ou supprimer ces données si 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, 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 Client dans laquelle elle identifie le Client, Google s'engage à :

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

b. en notifier le Client sans délai ; et

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

Le Client se chargera de répondre à la demande, y compris, si nécessaire, en utilisant 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 Client, Google s'engage à aider le Client à remplir ses obligations en vertu du Droit applicable relatif à la confidentialité (ou les obligations du responsable du traitement concerné si le Client 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 Client (ou responsable du traitement concerné) de respecter lesdites obligations, offrira au Client une coopération et une assistance supplémentaires raisonnables à sa demande.

10. Emplacements de traitement des données

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

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

11.2 *Informations sur les Sous-traitants indirects*. Les noms, emplacements 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 indirect, Google doit :

a. s'assurer par un contrat écrit que :

i. le Sous-traitant indirect n'accède aux Données du Client et ne les utilise qu'aux fins requises pour satisfaire aux obligations qui lui sont sous-traitées, et conformément au Contrat applicable (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 le présent Avenant 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 sous-traitées au Sous-traitant indirect, et de l'ensemble des actes et des manquements de ce dernier.

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 Client dudit engagement (y compris du nom, de l'emplacement et des activités du nouveau Sous-traitant indirect) au moins 30 jours avant que le nouveau Sous-traitant indirect ne commence à traiter les données du Client.

b. Dans un délai de 90 jours après avoir été informé de l'engagement d'un nouveau Sous-traitant indirect, le Client 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 ; Enregistrement des informations 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 Client en lien avec le traitement des Données du Client en vertu du Contrat. Elle peut être contactée tel que 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 Client, le Client 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 Client, Google invitera le tiers à contacter le Client.

13. Avis.

Tout avis envoyé en vertu du présent Avenant (y compris les notifications d'Incidents liés aux données) sera envoyé à l'Adresse courriel de notification. Le Client 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. le présent Avenant et le reste du Contrat, le présent Avenant prévaut.

En d'autres termes, si le Client a conclu plus d'un Contrat, le présent Avenant modifie chacun des Contrats séparément.

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

Annexe 1 : Objet et détails relatifs au traitement des données

Objet

Mise à disposition par Google des Services et des SAT (le cas échéant) au Client.

Durée du traitement

La Période de validité, plus la période allant de la fin de la Période de validité à la suppression de toutes les Données du Client par Google conformément aux présentes.

Nature et finalité du traitement

Google s'engage à traiter les Données à caractère personnel du Client aux fins de fournir les Services et SAT (le cas échéant) au Client conformément au présent Avenant.

Catégories de données

Données concernant des personnes et fournies à Google via les Services, par le Client (ou à sa demande) ou par les Utilisateurs finaux du Client.

Personnes concernées

Les Personnes concernées désignent les personnes à propos desquelles des données sont fournies à Google via les Services par le Client (ou à sa demande) ou par les Utilisateurs finaux du Client.

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 protéger les Mesures de sécurité définies dans la présente Annexe 2.

1. Centre de données et sécurité du réseau

(a) Centres de données.

Infrastructure. La société Google gère des centres de données répartis dans différentes zones géographiques. Elle stocke également toutes les données de production dans des centres de données physiquement protégés.

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 pouvoir être entretenus sans interruption de fonctionnement, 24h/24 et 7j/7. Dans la plupart des cas, une source d'alimentation 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, tels que des batteries d'alimentation sans coupure qui fournissent une protection électrique fiable en toutes circonstances, à savoir lors des baisses de tension, des coupures de courant, des surtensions, des sous-tensions et des conditions de fréquences hors tolérance touchant le service 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 des serveurs. Les serveurs Google utilisent un système d'implémentation Linux personnalisé pour l'environnement des applications. Les données sont stockées à l'aide d'algorithmes propriétaires afin 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 améliorer les produits de sécurité dans les environnements de production.

Continuité des activités. Google a conçu, planifie et teste régulièrement des plans de continuité des activités et des programmes de reprise après sinistre.

(*b) Réseaux et transmission*.

Transmission de données. En règle générale, les centres de données sont connectés via des connexions privées à haut débit afin 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 des technologies dédiées à ses systèmes externes.

Détection des intrusions. La détection des intrusions sert à fournir des informations sur les activités en cours liées à des attaques et sur la manière de réagir face aux incidents. La détection des intrusions de Google 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 exploite le chiffrement HTTPS (également appelé connexion SSL ou TLS). Les serveurs Google sont compatibles avec l'échange de clés cryptographiques éphémères Diffie-Hellman basé sur les courbes elliptiques. La signature est effectuée à l'aide des protocoles RSA et ECDSA. Ces méthodes de confidentialité persistante parfaite (PFS) permettent de protéger le trafic et de minimiser l'impact d'une clé compromise ou d'une percée cryptographique.

2. Contrôle sur site et contrôle d'accès.

(a) Contrôles sur site.

Gestion de la sécurité des centres de données sur site. Les centres de données Google bénéficient d'une équipe de gestion de la sécurité sur site chargée de toutes les fonctions de sécurité des centres de données physiques, 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 afin d'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. Toutes les personnes souhaitant pénétrer dans le centre de données doivent s'identifier et présenter une pièce d'identité au personnel gérant les opérations de 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 associés à la 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 physique, ainsi que les franchissements des portes du périmètre, des zones d'expédition et de réception, et 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, dont 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 par caméras. 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, qui doit obligatoirement suivre une formation à la sécurité dans le cadre de sa formation globale. Le personnel de sécurité des infrastructures de Google est 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 et les Utilisateurs finaux du Client doivent s'authentifier par l'intermédiaire d'un système d'authentification central ou d'authentification unique afin d'utiliser les Services.

Processus et règles d'accès aux données internes – Règlement d'accès. Les processus et les règles internes d'accès aux données de Google sont destinés à empêcher les personnes et les systèmes non autorisés d'accéder aux systèmes utilisés pour le traitement des Données du Client. 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, la modification ou la suppression des Données du Client 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 utilisent les certificats et clés de sécurité SSH. Ils sont conçus pour fournir à Google des mécanismes d'accès sécurisés et flexibles. Ces mécanismes n'octroient que les droits d'accès approuvés aux hôtes des sites, aux journaux, aux données et aux informations de configuration. Google requiert l'utilisation d'ID utilisateur uniques, de mots de passe sécurisés, de l'authentification à deux facteurs et de listes d'accès 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), les règles concernant les mots de passe qui sont au moins conformes aux pratiques standards de l'industrie sont appliquées. Ces pratiques standards incluent entre autres les restrictions 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 (ex. par

une sélection d'emplacement des données), Google réplique les Données du Client sur plusieurs centres de données dispersés géographiquement. Google isole également les Données du Client de manière logique. Le Client se voit confier le contrôle de certaines règles de partage des données. Ces règles, conformément aux fonctionnalités des Services, permettent au Client de déterminer les paramètres de partage de produit qui s'appliquent à ses Utilisateurs finaux pour des besoins particuliers. Le Client peut choisir d'utiliser la fonctionnalité de journalisation fournie par Google via les Services.

(b) *Disques hors service et règlement d'effacement des disques*. Les disques contenant des données peuvent rencontrer des problèmes de performances, des erreurs ou des pannes matérielles engendrant leur mise hors service (« Disque hors service »). Chaque Disque hors service est soumis à des processus de destruction des données (le « Règlement d'effacement des disques ») avant de quitter les locaux de Google en vue de sa réutilisation ou de sa destruction. Les Disques hors service sont effacés selon un processus en plusieurs étapes et validés par au moins deux experts indépendants. Les résultats du processus d'effacement sont consignés avec le numéro de série du Disque hors service à des fins de suivi. Enfin, le Disque hors service effacé est replacé dans l'inventaire afin de pouvoir être réutilisé et redéployé. Si, en raison d'une défaillance matérielle, le disque hors service ne peut pas être effacé, il est stocké de façon sécurisée jusqu'à ce que sa destruction soit possible. 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. Les employés chargés de manipuler les Données du Client doivent en outre se soumettre à des exigences supplémentaires adaptées à leur rôle (certifications, par exemple). Le personnel de Google n'est pas habilité à traiter les Données client sans autorisation.

5. Sous-traitants indirects 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 leur accès aux données et du champ d'application des services pour lesquels ils ont été recrutés. Une fois que Google a évalué les risques présentés par le Sous-traitant indirect, celui-ci est tenu d'accepter les conditions contractuelles appropriées en termes de sécurité et de confidentialité, sous réserve des conditions requises décrites à la Section 11.3 (Conditions requises pour l'engagement de Sous-traitants indirects).

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 Client.

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 2028 ; 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, tel que 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, sur une base autre que celle d'un 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 Client* » 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 Client ou les CCT (sous-traitant à sous-traitant, exportateur Google), selon le cas.

- « *CCT (responsable du traitement à sous-traitant)* » désigne les conditions disponibles à l'adresse https://cloud.google.com/terms/sccs/eu-c2p

- « *CCT (sous-traitant à responsable du traitement)* » désigne les conditions disponibles à l'adresse https://cloud.google.com/terms/sccs/eu-p2c

- « *CCT (sous-traitant à sous-traitant)* » désigne les conditions disponibles à l'adresse https://cloud.google.com/terms/sccs/eu-p2p

- « *CCT (sous-traitant à sous-traitant, exportateur Google)* » désigne les conditions disponibles à l'adresse https://cloud.google.com/terms/sccs/eu-p2p-google-exporter

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

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

b. qu'une Instruction va 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 un tel avis.

Si le Client est un sous-traitant, il transférera immédiatement au responsable du traitement concerné tout avis envoyé par Google en vertu de la présente section.

3. Droits d'audit du Client. Google peut donner l'autorisation au Client ou à un auditeur indépendant désigné par le Client d'effectuer des audits (y compris des inspections), conformément à la section 7.5.2(a) (Audit par le Client). Pendant ledit audit, Google s'engage à mettre à disposition toutes les informations nécessaires permettant de démontrer sa conformité à ses obligations en vertu du présent Avenant et de contribuer à l'audit tel que décrit à la Section 7.5 (Examens et Audits de conformité) et dans la présente section.

4. Transferts de données.

4.1 *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 Client dans un Pays approprié ou de leur transfert vers un Pays approprié. Si les Données à caractère personnel du Client 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 Client en vertu de la Section 4.2 (Certification par des Clients 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, Google s'engage à informer le Client 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 informe le Client que Google 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 de Google aux Sous-traitants indirects ; et

b. de plus, si l'adresse de facturation du Client ne se situe pas dans un Pays approprié, les CCT (sous-traitant à responsable du traitement) s'appliquent (que le Client soit un responsable du traitement ou un sous-traitant) en ce qui concerne lesdits Transferts limités entre Google et le Client ; 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 Client est un responsable du traitement ou un sous-traitant) en ce qui concerne lesdits Transferts limités entre Google et le Client.

4.2 *Certification par des Clients basés hors de la région EMEA*. Si l'adresse de facturation du Client se situe en dehors de la région EMEA et que le traitement des Données à caractère personnel du Client est régi par la Législation européenne sur la protection des données, le Client 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 Client des informations pertinentes aux Transferts limités, Contrôles de sécurité supplémentaires et autres mesures de protection complémentaires :

a. tel que décrit à la Section 7.5.1 (Examen de la Documentation relative à la sécurité) ;

b. dans 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 Client 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 Client (ou un auditeur indépendant désigné par le Client) à effectuer des audits tel que 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 Client s'engage à transmettre sans délai ni retard injustifié 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 Client conclut que les Données à caractère personnel du Client 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.

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

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

5. Conditions requises pour engager des Sous-traitants indirects. La Législation européenne sur la protection des données veut que Google veille, au moyen d'un contrat écrit, à ce que les obligations en matière de protection de données énoncées dans les présentes et reprises à l'Article 28(3) du RGPD 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.

- « *Données à caractère personnel du Client* » inclut 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 Client conformément au CCPA et sans porter préjudice aux obligations de Google en vertu de la Section 5.2 (Conformité aux Instructions du Client), Google s'engage, sauf si le CCPA le permet, à :

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

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

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

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

c. ne pas combiner ni mettre à jour les Données à caractère personnel du Client 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 porter préjudice à ses obligations en vertu de la Section 5.2 (Conformité aux Instructions du Client) ni à tout autre droit ou obligation de quelconque partie en vertu du Contrat

applicable, Google s'engage, sauf si le droit applicable le lui interdit, à informer le Client s'il estime ne pas être en mesure de satisfaire à ses obligations en vertu du CCPA.

4. Intervention du Client. Si Google informe le Client de toute utilisation non autorisée des Données à caractère personnel du Client, y compris en vertu de la Section 3 (Conformité) de la présente sous-section ou de la Section 7.2.1 (Notification d'incident), le Client peut prendre les mesures raisonnables et appropriées pour mettre fin à une telle utilisation non autorisée ou y remédier :

a. en prenant les mesures recommandées par Google conformément à la Section 7.2.2 (Détails des incidents liés aux données), le cas échéant ; ou

b. en exerçant ses droits en vertu de la Section 7.5.2 (Audit par le Client) ou 9.1 (Accès ; Rectification ; Traitement restreint ; 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 en vertu de la Législation turque sur la protection des données.

2. Transferts de données.

2.1 *Conditions supplémentaires*. Si l'adresse de facturation du Client se trouve en Turquie et que Google met à disposition du Client pour acceptation des conditions supplémentaires facultatives (y compris les CCT turques) en lien avec les transferts de Données à caractère personnel du Client en vertu de la Législation turque sur la protection des données, ces conditions viendront compléter le présent Avenant à compter de la date où elles sont notifiées 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 en atteste le Client à Google.

2.2 *Notification à l'autorité compétente*. Si le Client signe des CCT turques en vertu 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 des 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 *Audits des CCT*. Si le Client signe des CCT turques en vertu de la présente Section 2 (Transferts de données), Google autorisera le Client (ou un auditeur indépendant désigné par le Client) à effectuer des audits tel que décrit dans lesdites CCT et, pendant un audit, mettra à disposition toutes les informations requises par lesdites CCT 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 Client conclut que les Données à caractère personnel du Client 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 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 en vertu de 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 le présent Avenant dès lors que le Client 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 équivalent à « responsable du traitement », « données à caractère personnel », « traitement » et « sous-traitant » utilisé dans le présent Avenant a la signification qui lui est attribuée dans la Loi israélienne sur la protection de la confidentialité.

3. Droits d'audit du Client. Google peut donner l'autorisation au Client ou à un auditeur indépendant désigné par le Client d'effectuer des audits (y compris des inspections), conformément à la section 7.5.2(a) (Audit par le Client).

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 Client 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 Client.

- « *Données du Client* », si le terme n'est pas défini dans le Contrat, désigne les données fournies à Google par le Client ou ses Utilisateurs finaux via Google Cloud Platform sous le Compte, ainsi que les données que le Client ou ses Utilisateurs finaux dérivent de ces données via leur utilisation de Google Cloud Platform.

- « *Google Cloud Platform* » désigne les services Google Cloud Platform décrits à l'adresse https://cloud.google.com/terms/services, à l'exclusion des éventuelles Offres tierces.

- « *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 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 avec PCI DSS.

3. Emplacements des centres de données. Les emplacements des centres de données de Google Cloud Platform sont décrits à l'adresse 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 à l'adresse 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 pertinentes aux Transferts limités, Contrôles de sécurité supplémentaires et autres mesures de protection complémentaires sont disponibles à l'adresse 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 conçue avec certaines caractéristiques distinctes.

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

- La définition de « Auditeur tiers de Google » est remplacée par la suivante :

    - « *Auditeur tiers de Google* » désigne un auditeur tiers qualifié et indépendant désigné par Google ou par un Sous-traitant indirect de la solution Bare Metal et dont Google divulguera l'identité alors connue au Client à la demande de ce dernier.

- Les formulations suivantes ont été supprimées :

    - Dans la Section 7.1.1 (Mesures de sécurité de Google), la phrase « pour permettre le chiffrement des Données du Client » ;

- Dans l'Annexe 2 (Mesures de sécurité), les sous-sections de la Section 1(a) intitulées « Systèmes d'exploitation serveur » et « Continuité de l'activité » ;

- Dans l'Annexe 2, les sous-sections de la Section 1(b) intitulées « Surface d'attaque externe », « Détection des intrusions » et « Technologies de chiffrement » ; et

- 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 du Client (par exemple, par une sélection d'emplacement des données), Google réplique les Données du Client sur plusieurs centres de données dispersés géographiquement.

2. Certifications de conformité et Rapports SOC. Google ou son Sous-traitant indirect s'engage à maintenir au minimum les normes suivantes (ou une alternative équivalente ou améliorée) 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 avec 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 relative à 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 Client les Certifications de conformité BMS et les Rapports SOC BMS en vue de leur examen et, si le Client est un sous-traitant, s'engage à permettre au Client 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 Client. Sans limiter les obligations expresses de Google en ce qui concerne la solution Bare Metal, le Client s'engage à prendre des mesures raisonnables afin de protéger et préserver la sécurité des Données du Client et de tout autre contenu stockés sur la solution Bare Metal ou traités via celle-ci.

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 autre que matérielle ;

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

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

Le Client 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, et la sauvegarde des Systèmes d'exploitation, Données du Client, logiciels et applications que le Client utilise, importe ou héberge sur la solution Bare Metal.

Cloud NGFW (Google Cloud Platform)

L'édition de Cloud NGFW « 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 Client) 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 du trafic réseau soumis(e) à des fins de SAT et désigné(e) par CNE comme une menace de sécurité, à condition que le fichier ou la capture de paquet du trafic réseau n'inclue pas de Données à caractère personnel du Client.

Google Distributed Cloud connecté (Google Cloud Platform)

Google Distributed Cloud connecté 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 Google Distributed Cloud connecté :

- 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*. À la date d'expiration de la Période de validité, le Client ordonne à Google la suppression de toutes les Données du Client restantes (y compris les copies existantes) des systèmes de Google, en vertu de la loi applicable. Si le Client souhaite conserver certaines Données du Client à l'expiration de la Période de validité, il peut exporter ou copier ces données avant 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 (Stockage des données et installations de traitement) : « ou quelconque pays où se trouve une Adresse de 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 Client ne sont stockées que sur l'Équipement devant être déployé à une Adresse du client.

      Systèmes d'exploitation des serveurs. Les serveurs Google utilisent un système d'implémentation Linux personnalisé pour l'environnement des applications. Google applique un processus de revue de code afin d'accroître la sécurité du code utilisé pour fournir Google Distributed Cloud connecté et améliorer les produits de sécurité dans les environnements de production Google Distributed Cloud connecté.

      Technologies de chiffrement. Google exploite le chiffrement HTTPS (également appelé connexion SSL ou TLS) et autorise le chiffrement des données en transit. Les serveurs Google sont compatibles avec l'échange de clés cryptographiques éphémères Diffie-Hellman basé sur les courbes elliptiques. La signature est effectuée à l'aide des protocoles RSA et ECDSA. Ces méthodes de confidentialité persistante parfaite (PFS) permettent de protéger le trafic et de minimiser l'impact d'une clé compromise ou d'une percée cryptographique. Google exploite également le chiffrement des données au repos avec au minimum AES128 ou un algorithme similaire. Google Distributed Cloud connecté bénéficie d'une intégration CMEK. Des informations complémentaires sont accessibles à l'adresse https://cloud.google.com/kms/docs/cmek.

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

      Stockage lié. Le stockage des Données du Client 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 sur site et contrôle d'accès) 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 relative à 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 Google Distributed Cloud connecté.

Multicloud géré par Google (Google Cloud Platform)

Les Services multicloud 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 disponibles à l'adresse https://cloud.google.com/terms/mcs-data-processing-terms.

2. Conditions relatives au traitement des données pour 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 se peut que Google n'ait pas accès à l'environnement VMware du Client ou ne puisse pas chiffrer les données à caractère personnel dans l'environnement VMware du Client.

NetApp Volumes (Google Cloud Platform)

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

- La définition de « Auditeur tiers de Google » est remplacée par la suivante :
    - « *Auditeur tiers de Google* » désigne un auditeur tiers qualifié et indépendant nommé par Google ou par un Sous-traitant indirect de NetApp Volumes et dont Google divulguera l'identité au Client à la demande de ce dernier.
- La Section 3(a) (Stockage, isolation et journalisation des données) 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 (par exemple, par une sélection d'emplacement des données), Google réplique les Données du Client sur plusieurs centres de données dispersés géographiquement. Google isole également les Données du Client de manière logique. Le Client se voit confier le contrôle de certaines règles de partage des données. Ces règles, conformément aux fonctionnalités des Services, permettent au Client de déterminer les paramètres de partage de produit qui s'appliquent à ses Utilisateurs finaux pour des besoins particuliers. Le Client 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'engage à obtenir au minimum les certifications et rapports suivants (ou une alternative équivalente ou améliorée) pour NetApp Volumes :

a. un certificat pour ISO 27001 et une Attestation de conformité avec 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 relative à 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 Client les

Certifications de conformité NetApp et les Rapports SOC NetApp en vue de leur examen et, si le Client est un sous-traitant, s'engage à permettre au Client de demander 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).

Google Workspace et Cloud Identity

1. Définitions supplémentaires.

- « *Compte* », s'il n'est pas défini dans le Contrat, désigne le compte Google Workspace ou Cloud Identity du Client.
- « *Cloud Identity* », lorsqu'il est acheté avec un Contrat autonome et ne fait pas partie de Google Cloud Platform ou Google Workspace, signifie les Services Cloud Identity décrits à l'adresse https://cloud.google.com/terms/identity/user-features.
- « *Données du Client* », si le terme n'est pas défini dans le Contrat, désigne les données soumises, stockées, envoyées ou reçues par le Client ou ses Utilisateurs finaux ou en leur nom via Google Workspace ou Cloud Identity sous le Compte.
- « *Google Workspace* » désigne les Services Google Workspace ou Google Workspace for Education décrits à l'adresse https://workspace.google.com/terms/user_features.html, selon le cas.

2. Produits complémentaires. Si Google, à sa discrétion, met des Produits complémentaires à disposition du Client pour une utilisation avec Google Workspace ou Cloud Identity conformément aux Conditions relatives aux Produits complémentaires :

a. le Client peut activer ou désactiver les Produits complémentaires via la Console d'administration et ne sera pas tenu d'utiliser les Produits complémentaires afin de pouvoir utiliser Google Workspace ou Cloud Identity ; et

b. si le Client choisit d'installer des Produits complémentaires ou de les utiliser avec Google Workspace ou Cloud Identity, les Produits complémentaires peuvent accéder aux Données du Client en fonction des besoins pour interopérer avec Google Workspace ou Cloud Identity, selon le cas.

En d'autres termes, le présent Avenant ne s'applique pas au traitement des données à caractère personnel en relation avec la fourniture de tout Produit supplémentaire installé ou utilisé par le Client, y compris les données à caractère personnel transmises vers ou à partir de ce Produit supplémentaire.

3. Certifications de conformité. Les Certifications de conformité pour les Services audités de Google Workspace et Cloud Identity incluent également les certificats pour ISO 27017 et ISO 27018.

4. Emplacements des centres de données. Les emplacements des centres de données Google Workspace et Cloud Identity sont décrits à l'adresse https://www.google.com/about/datacenters/locations/.

5. Informations sur les Sous-traitants indirects. Les noms, les emplacements et les activités des Sous-traitants indirects de Google Workspace et Cloud Identity sont décrits à l'adresse https://workspace.google.com/intl/en/terms/subprocessors.html.

6. Équipe chargée de la protection des données dans le cloud. L'Équipe chargée de la protection des données pour Google Workspace et Cloud Identity peut être contactée à l'adresse https://support.google.com/cloud/contact/dpo (lorsque les administrateurs sont connectés à leur compte administrateur).

7. Mesures de sécurité supplémentaires. Pour Google Workspace et Cloud Identity :

a. Google sépare logiquement les données de chaque Utilisateur final des données des autres Utilisateurs finaux ; et

b. les données d'un Utilisateur final authentifié ne seront pas affichées à un autre Utilisateur final (sauf si le premier ou un administrateur autorise le partage de ces données).

8. Informations sur les Transferts limités. Des informations pertinentes aux Transferts limités, Contrôles de sécurité supplémentaires et autres mesures de protection complémentaires sont disponibles à l'adresse https://cloud.google.com/privacy.

9. Avenant relatif aux données du Service. Si Google met à disposition du Client, pour acceptation, un Avenant relatif aux données du Service facultatif en lien avec le présent Avenant, la disponibilité de cet avenant facultatif constitue une « Mise à jour DPA » si un tel terme est défini dans tout Avenant relatif aux données du Service précédemment accepté par le Client.

10. Conditions spécifiques des Services.

AppSheet (Google Workspace)

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

- Le paragraphe intitulé « Systèmes d'exploitation des serveurs » de la Section 1(a) de l'Annexe 2 (Mesures de sécurité) est remplacé par ce qui suit :
    - *Systèmes d'exploitation des serveurs*. Les serveurs Google utilisent un système d'implémentation Linux personnalisé pour l'environnement des applications.

2. Emplacements des centres de données supplémentaires. Les emplacements des centres de données supplémentaires pour AppSheet sont décrits à l'adresse https://cloud.google.com/about/locations/.

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 disponibles à l'adresse 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, dont les API associées) qui permet aux entreprises d'analyser des données et de définir des métriques commerciales pour plusieurs sources de données qui ont été fournies au Client 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 Client a effectué l'achat via un revendeur ou une place de marché en ligne ou qu'il utilise Looker dans le cadre d'un essai ou à des fins d'évaluation en vertu 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 d'« Adresse courriel de notification » est remplacée par la suivante :

    - « Adresse courriel de notification » désigne la ou les adresse(s) courriel indiquée(s) par le Client 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 disponibles à l'adresse https://cloud.google.com/terms/looker/legal/sccs/eu-c2p

    - « *CCT (sous-traitant à responsable du traitement)* » désigne les conditions disponibles à l'adresse https://cloud.google.com/terms/looker/legal/sccs/eu-p2c

    - « *CCT (sous-traitant à sous-traitant)* » désigne les conditions disponibles à l'adresse https://cloud.google.com/terms/looker/legal/sccs/eu-p2p

- « *CCT (sous-traitant à sous-traitant, exportateur Google)* » désigne les conditions disponibles à l'adresse https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group

- Les mots suivants sont ajoutés à la fin de la Section 10.1 (Installations de stockage et traitement des données) : « ou quelconque endroit où les fournisseurs tiers de services multicloud disposent d'installations. »

3. Responsabilité supplémentaire du Client en termes de sécurité. Le Client est responsable de la sécurité de l'environnement, des bases de données et de la configuration de Looker (original) du Client, à l'exception des systèmes gérés et contrôlés par Google.

4. Certifications de conformité et Rapports SOC. Les Certifications de conformité et les Rapport 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. Absence de certification par des Clients basés hors de la région EMEA. Le Client 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 des Clients 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 aux Transferts limités, Contrôles de sécurité supplémentaires et autres mesures de protection complémentaires sont disponibles à l'adresse 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 aux adresses 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 gérés par Google nécessitent des infrastructures tierces et ont été conçus avec certaines caractéristiques distinctes.

9.1 *Conditions relatives au traitement des données pour 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 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 Client, le Client 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 Client de fournir et mettre à jour lesdites informations par d'autres moyens.

12. Mesures de sécurité des applications supplémentaires. Google s'engage à mettre en œuvre et garantir 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 pour aider 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 Client contrôlent les accès aux applications par le personnel de Google afin de fournir l'assistance technique requise par le Client ou ses Utilisateurs finaux.

Services SecOps

1. Définitions supplémentaires.

- « *Compte* », s'il n'est pas défini dans le Contrat, désigne le compte des Services SecOps ou le compte Google Cloud Platform du Client, selon le cas.
- « *Données du Client* », si le terme n'est pas défini dans le Contrat, signifie les données fournies à Google par le Client ou ses Utilisateurs finaux via les Services SecOps sous le Compte ou, pour les Services Mandiant Consulting et les Services gérés Mandiant, en lien avec les Services SecOps récepteurs.
- « *Fournisseur engagé par le Client* » désigne un fournisseur de services (qui peut inclure un sous-traitant ou un sous-traitant indirect) directement engagé par le Client selon un Contrat séparé entre le Client et ce fournisseur.
- « *Services SecOps* » désigne les Services SecOps décrits à l'adresse https://cloud.google.com/terms/secops/services, à l'exception de toute Offre tierce.
- « *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 (c) 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 Client 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 pertinent disponible à l'adresse https://cloud.google.com/security/compliance/secops/services-in-scope. Google ne peut effacer de Services SecOps de cette URL que s'ils ont été arrêtés conformément au Contrat applicable.

- 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 disponibles à l'adresse https://cloud.google.com/terms/sccs/eu-c2p ;

  - « CCT (sous-traitant à responsable du traitement) » désigne les conditions disponibles à l'adresse https://cloud.google.com/terms/secops/sccs/eu-p2c ;

  - « CCT (sous-traitant à sous-traitant) » désigne les conditions disponibles à l'adresse https://cloud.google.com/terms/secops/sccs/eu-p2p ; et

  - « CCT (sous-traitant à sous-traitant, exportateur Google) » désigne les conditions disponibles à l'adresse https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter.

- La Section 6.1 (Suppression par le Client) est modifiée comme suit :

  - 6.1 **Suppression par le Client**. Google permet au Client de supprimer les Données du Client au cours de la Période de validité et d'une manière conforme aux fonctionnalités des Services ou à la demande. Si le Client utilise les Services pour supprimer des Données du Client au cours de la Période de validité et que ces Données du Client ne peuvent pas être récupérées par le Client, ou si le Client demande la suppression de Données du Client au cours de la Période de validité, cette utilisation ou cette demande constituera une instruction donnée à Google de supprimer les Données du Client concernées des systèmes de Google en vertu de la loi applicable. Google s'engage à respecter cette Instruction 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 de ces données.

- 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 à l'adresse 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 se réserve le droit d'ajouter des normes à tout moment. Google se réserve le droit de trouver une alternative équivalente ou améliorée à une Certification de conformité ou à un Rapport SOC.

- La Section 9.1 (Accès ; Rectification ; Traitement restreint ; Portabilité) est modifiée comme suit :

    9.1 **Accès ; Rectification ; Traitement restreint ; Portabilité**. Au cours de la Période de validité, Google, tout en respectant les fonctionnalités des Services, s'engage à permettre au Client d'accéder aux Données du Client, de les rectifier et d'en restreindre le traitement, y compris tel que décrit dans la Section 6.1 (Suppression par le Client), et d'exporter les Données du Client sur demande. Si le Client découvre que des Données à caractère personnel du Client sont inexactes ou obsolètes, il est responsable d'en informer Google et Google aidera le Client à modifier ces données si cela est requis par le Droit applicable relatif à la confidentialité.

3. Emplacements des centres de données. Les emplacements des centres de données des Services SecOps sont décrits à l'adresse https://cloud.google.com/terms/secops/data-residency.

4. Absence de certification par des Clients basés hors de la région EMEA. Le Client 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 des Clients 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 à l'adresse 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 proposé de temps en temps par Google).

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 Client, le Client 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 Client de fournir et mettre à jour lesdites informations par d'autres moyens.

8. Conditions spécifiques des Services.

Services Mandiant Consulting et Services gérés Mandiant

Les Services Mandiant Consulting et les Services gérés Mandiant fournissent des services de conseil et d'implémentation (y compris la réponse aux incidents, la préparation stratégique et l'assurance technique pour limiter les menaces et réduire les risques liés aux incidents) et des services gérés de détection et de réponse et ont été conçus avec certaines caractéristiques distinctes.

1. Modifications. L'Avenant est modifié comme suit seulement en ce qui concerne les Services Mandiant Consulting et les Services gérés Mandiant :

- La définition d'« Incident lié aux données » est remplacée par ce qui suit :
    - En d'autres termes, un Incident lié aux données exclut les incidents qui font l'objet des Services Mandiant Consulting et/ou des Services gérés Mandiant, le cas échéant.
- La Section 5.2(b)(i) (Conformité avec les Instructions du Client) est remplacée par ce qui suit :
    - i. Utilisation des Services par le Client ; et
- La seconde phrase de la Section 7.1.1 (Mesures de sécurité de Google) est modifiée comme suit :
    - Les Mesures de sécurité peuvent inclure (le cas échéant) des mesures pour permettre le chiffrement des Données du Client ; pour garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de Google ; pour rétablir rapidement l'accès aux Données du Client à la suite d'un incident ; et pour tester régulièrement leur efficacité.
- La Section 7.3.1(b) est modifiée comme suit :
    - b. l'administration, la gestion des accès et la sécurisation des identifiants d'authentification du compte, des systèmes, du logiciel, des réseaux et des appareils que le Client utilise pour recevoir les Services Mandiant Consulting et/ou les Services gérés Mandiant, selon le contexte, ou pour autoriser Google à y accéder afin de les fournir ;
- Les nouvelles Sections 7.3.1(d) et (e) sont ajoutées comme suit :
    - d. la limitation de la quantité de Données du Client fournie par le Client ou en son nom à Google ; et

- e. dans la mesure où l'accès de Google aux Données du Client se trouve sous le contrôle du Client, la révocation dudit accès lorsque Google a terminé les Services Mandiant Consulting et/ou les Services gérés Mandiant, selon le cas.

- L'Annexe 2 (Mesures de sécurité) est remplacée comme suit :

    - Annexe 2 : Mesures techniques et organisationnelles supplémentaires

      1. Environnement contrôlé par le client. Google accédera aux Données à caractère personnel du Client fournies à Google par le Client ou en son nom et les traitera uniquement via un compte ou un environnement contrôlé ou approuvé par le Client.

      2. Processus et règles d'accès aux données internes – Règlement d'accès. Les processus et les règles d'accès aux données de Google sont destinés à empêcher les personnes et/ou les systèmes non autorisés d'accéder aux systèmes utilisés pour le traitement des Données du Client. Google (i) ne permet qu'aux personnes autorisées d'accéder aux données auxquelles elles sont en droit d'accéder ; et (ii) prend des mesures pour empêcher la lecture, la copie, la modification ou la suppression des données à caractère personnel sans autorisation lors de leur traitement et en cours d'utilisation. L'octroi et la modification des droits d'accès par Google sont basés sur la fourniture par le Client à Google de l'accès utilisateur final à son compte ou son environnement.

      3. Personnel 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 doit respecter un accord de confidentialité ainsi que les règles de Google en matière de confidentialité et de respect de la vie privée, dont il doit par ailleurs accuser réception. Il reçoit aussi une formation à la sécurité. Les employés chargés de manipuler les Données du Client doivent en outre se soumettre à des exigences supplémentaires adaptées à leur rôle (certifications, par exemple). Le personnel de Google n'est pas habilité à traiter les Données client sans autorisation.

      4. Mesures de sécurité supplémentaires. Google et le Client peuvent inclure des mesures de sécurité supplémentaires dans le Formulaire de commande applicable, y compris tout Cahier des charges joint, pour les Services Mandiant Consulting et/ou les Services gérés Mandiant, le cas échéant.

2. Fournisseur engagé par le Client. À des fins de clarté, et sans limiter les obligations de Google en vertu des Sections 7 (Sécurité des données) ou 11 (Sous-traitants indirects), l'Annexe 2 (Mesures de sécurité) ne décrit pas les mesures de sécurité ni les contrôles mis en œuvre ou fourni par le Client ou les Fournisseurs engagés par le Client.

Services d'implémentation

1. Définitions supplémentaires.

- « *Données du Client* » désigne les données auxquelles le Client autorise Google à accéder sur les Systèmes gérés par le client.
- « *Systèmes gérés par le Client* » désigne les éléments suivants, tels qu'utilisés par le Client pour recevoir les Services d'implémentation : (a) les Instances gérées par le Client des Services Google Cloud ou de Services Cloud tiers ; et (b) tout matériel ou logiciel hébergé ou géré dans l'environnement sur site du Client.
- « *Services Google Cloud* » désigne tous les Services décrits dans la présente Annexe 4 (Produits spécifiques), autres que les Services d'implémentation, les Services Mandiant Consulting et les Services gérés Mandiant.
- « *Personnel de Google* » désigne les employés et sous-traitants de Google engagés pour fournir les Services d'implémentation.
- « *Services d'implémentation* » désigne les services de conseil et d'implémentation fournis par les employés et sous-traitants de Google pour l'exécution des Services Google Cloud tel que décrit dans le Contrat, y compris dans un Formulaire de commande ou un Cahier des charges.

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

- La définition de « Contrôles de sécurité supplémentaires » est effacée.
- La définition d'« Incident lié aux données » est remplacée par ce qui suit :
    - « *Incident lié aux données* » désigne une violation de la Section 7.1 (Mesures et contrôle de sécurité, et assistance de Google en matière de sécurité) par le Personnel de Google, entraînant, de manière accidentelle ou illégale, la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés à des Données à caractère personnel du Client.
- Sous réserve du reste de cette Section, le terme « Données du Client » est remplacé par « Données à caractère personnel du Client » lorsqu'il est utilisé (a) dans la Section 2 (Définitions) dans la définition de « Sous-traitant indirect », et (b) dans d'autres Sections du présent Avenant. En d'autres termes, les autres définitions de la Section 2 (Définitions) restent inchangées.
- La Section 3 (Durée) est remplacée par ce qui suit :
    - **3. Durée**. Quand bien même le Contrat applicable serait résilié ou arrivé à expiration, le présent Avenant reste de plein effet jusqu'à ce que Google n'ait plus accès aux

Données à caractère personnel du Client, et expire automatiquement au même moment.

- La Section 6 (Suppression des données) est remplacée par ce qui suit :
    - **6. Suppression des Données.** À l'expiration de la Période de validité, le Client (a) déterminera s'il est nécessaire de supprimer tout ou partie des Données à caractère personnel du Client, et (b) sera responsable d'une telle suppression.
- La seconde phrase de la Section 7.1.1 (Mesures de sécurité de Google) est remplacée par ce qui suit :
    - « Les Mesures de sécurité peuvent inclure (le cas échéant) des mesures pour permettre le chiffrement des Données du Client ; pour garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de Google ; pour rétablir rapidement l'accès aux Données du Client à la suite d'un incident ; et pour tester régulièrement leur efficacité. »
- La Section 7.1.3 (Contrôles de sécurité supplémentaires) est supprimée, ainsi que toutes les autres références à cette section.
- La Section 9.1 (Accès ; Rectification ; Traitement restreint ; Portabilité) est remplacée par ce qui suit :
    - 9.1 *Accès ; Rectification ; Traitement restreint ; Portabilité*. Le Client sera responsable d'utiliser la fonctionnalité des Systèmes gérés par le Client pour accéder aux Données à caractère personnel du Client, les rectifier et en limiter le traitement, y compris si le Client découvre que les Données à caractère personnel du Client sont inexactes ou obsolètes et est tenu par le Droit applicable relatif à la confidentialité de les rectifier ou de supprimer ces données.
- La Section 11.4 (Possibilité de s'opposer à des Sous-traitants indirects) est remplacée par ce qui suit :
    - 11.4 *Possibilité de s'opposer à des Sous-traitants indirects*. Lorsqu'un nouveau Sous-traitant indirect est engagé au cours de la Période de validité, Google informe le Client dudit engagement avant le début du traitement des Données à caractère personnel du Client Le Client peut s'opposer au nouveau Sous-traitant indirect en en informant Google et, dans ce cas, les parties s'efforceront de bonne foi de déterminer une alternative mutuellement acceptable.
- L'Annexe 1 (Objet et détails relatifs au traitement des données) est modifiée comme suit :
    - La section « Durée du traitement » est remplacée par ce qui suit :

- *« Durée du traitement*. La Période de validité, plus (le cas échéant) la période allant de la fin de la Période de validité à l'expiration de l'accès de Google à toutes les Données à caractère personnel du Client. »

- Les mots « fournis à Google via les Services » dans les sections « Catégories de données » et « Personnes concernées » sont remplacés par « mis à disposition de Google en lien avec les Services ».

- L'Annexe 2 (Mesures de sécurité) est remplacée comme suit :

  - **Annexe 2 : Mesures de sécurité**

    1. Systèmes gérés par le Client. Le Personnel de Google accèdera aux Données à caractère personnel du Client et les traitera uniquement sur les Systèmes gérés par le Client. Si ces systèmes incluent les Services Google Cloud, l'utilisation des Services Google Cloud par le Client reste régie par le contrat applicable à ces services.

    2. Contrôle des accès. Les processus et les règles internes d'accès aux données de Google sont destinés à empêcher les personnes et/ou les systèmes non autorisés d'accéder aux Services Google Cloud utilisés pour le traitement des données à caractère personnel. Les Règles Google (i) autorisent uniquement le Personnel de Google à accéder aux données auxquelles il est en droit d'accéder ; et (ii) empêchent le Personnel de Google de lire, copier, modifier ou supprimer des Données à caractère personnel du Client sans autorisation lors de leur traitement, en cours d'utilisation et après leur enregistrement. Le Client contrôle le provisionnement ou la modification des droits d'accès des utilisateurs finaux aux Systèmes gérés par le Client. Si ces systèmes incluent les Services Google Cloud, les informations sur les outils de workflow qui conservent les enregistrements d'audit de toutes les modifications et les journaux d'accès au système sont stipulés dans le Contrat pour les Services Google Cloud applicables.

    3. Personnel 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. Les employés chargés de traiter les Données à caractère personnel du Client doivent en outre se soumettre à des exigences supplémentaires adaptées à leur rôle (certifications, par exemple).

    4. Mesures de sécurité supplémentaires. Google et le Client peuvent inclure des mesures de sécurité supplémentaires dans le Contrat, y compris dans le Formulaire de commande ou un Cahier des charges.

5. Sous-traitants indirects 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 leur accès aux données et du champ d'application des services pour lesquels ils ont été recrutés. Une fois que Google a évalué les risques présentés par le Sous-traitant indirect, celui-ci est tenu d'accepter les conditions contractuelles appropriées en termes de sécurité et de confidentialité, sous réserve des conditions requises décrites à la Section 11.3 (Conditions requises pour l'engagement de Sous-traitants indirects).

3. Responsabilités du Client en matière de sécurité. Outre ses obligations au titre de la Section 7.3.1 (Responsabilités du Client en matière de sécurité), le Client est responsable de ce qui suit :

- administration, gestion des accès et sécurisation des Systèmes gérés par le Client, y compris la limitation de l'accès du Personnel de Google aux Données à caractère personnel du Client dans la mesure du possible et annulation de l'accès à la cessation des Services d'implémentation ; et

- implémentation de toutes les recommandations de sécurité fournies par écrit par Google au Client en ce qui concerne les Systèmes gérés par le Client.

4. Certification de conformité. Google maintiendra des certificats pour ISO 27001, ISO 27017 et ISO 27018 couvrant les Services d'implémentation fournis avec Google Cloud Platform et Google Workspace (les « *Certifications de conformité des Services d'implémentation* »). Google peut ajouter des normes à tout moment. Google se réserve le droit de trouver une alternative équivalente ou améliorée à une Certification de conformité des Services d'implémentation.

5. Examen de la Certification de conformité. Pour démontrer qu'il se conforme à ses obligations au titre du présent Avenant, Google s'engage à mettre à la disposition du Client la Certification de conformité des Services d'implémentation en vue de leur examen et, si le Client est un sous-traitant, s'engage à permettre au Client de demander accès à la Certification de conformité des Services d'implémentation pour le responsable du traitement concerné.

6. Emplacements de traitement des données. Les Données à caractère personnel du Client peuvent être traitées dans tout pays où Google fournit des Services d'implémentation ou où le Client possède des Systèmes gérés par le Client.

7. Absence de certification par des Clients basés hors de la région EMEA. Le Client 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 des Clients 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 d'implémentation.

8. Informations sur les Sous-traitants indirects. Les Sous-traitants indirects pour les Services d'implémentation seront identifiés (en tant que sous-traitants) dans un Formulaire de commande, un Cahier des charges ou toute autre confirmation applicable fourni(e) au Client avant le début des Services d'implémentation, ou seront des Sociétés affiliées de Google. Google mettra aussi à

disposition du Client les noms, emplacements et activités des Sous-traitants indirects pour les Services d'implémentation, sur demande.

9. 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 Client, le Client 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 Client de fournir et mettre à jour lesdites informations par d'autres moyens.

Google Cloud Skills Boost pour les Entreprises

1. Définitions supplémentaires.

- « *Compte* », s'il n'est pas défini dans le Contrat, désigne le compte Google Cloud Skills Boost pour les Entreprises du Client.
- « *GCSBO* » désigne les services d'enseignement, de formation et d'apprentissage ainsi que tout contenu fournis via https://www.cloudskillsboost.google/ (ou tout autre site Web géré ou contrôlé par Google et utilisé aux fins de Google Cloud Skills Boost pour les Entreprises).
- « *SAT* » désigne les services d'assistance technique que Google, à sa discrétion, peut fournir au Client.

2. Modifications. Le présent Avenant est modifié comme suit en ce qui concerne GCSBO :

- 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 Client 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.
- 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 disponibles à l'adresse https://cloud.google.com/terms/looker/legal/sccs/eu-c2p ;
    - « CCT (sous-traitant à responsable du traitement) » désigne les conditions disponibles à l'adresse https://cloud.google.com/terms/looker/legal/sccs/eu-p2c ;
    - « CCT (sous-traitant à sous-traitant) » désigne les conditions disponibles à l'adresse https://cloud.google.com/terms/looker/legal/sccs/eu-p2p ;

- « CCT (sous-traitant à sous-traitant, exportateur Google) » désigne les conditions disponibles à l'adresse https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group.

3. Emplacements des centres de données. Les emplacements des centres de données de Google Cloud Platform sont décrits à l'adresse https://cloud.google.com/about/locations/.

4. Absence de certification par des Clients basés hors de la région EMEA. Le Client 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 des Clients 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 GCBSO.

5. Informations sur les Sous-traitants indirects. Les noms, emplacements et activités des Sous-traitants indirects pour GCBSO sont décrits aux adresses :

a. https://cloud.google.com/terms/skillsboost-organizations/subprocessors ; et

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

6. Équipe chargée de la protection des données dans le cloud. L'Équipe chargée de la protection des données pour GCBSO peut être contactée à l'adresse https://support.google.com/cloud/contact/dpo (et/ou via tout autre moyen proposé de temps en temps par Google).

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 Client, le Client 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 Client 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 :

9 avril 2024 30 juin 2022 24 septembre 2021 19 août 2020 10 août 2020 17 juillet 2020 11 octobre 2019 1er octobre 2019 25 mai 2018 13 mars 2018 9 novembre 2017 11 octobre 2017 7 février 2017 6 octobre 2016

Précédentes versions de l'Avenant relatif au traitement des données :

7 juillet 2022 24 septembre 2021 27 mai 2021 29 octobre 2019 25 mai 2018 25 avril 2018 11 juillet 2017 28 novembre 2016 7 janvier 2016 24 avril 2015 1er avril 2014 14 novembre 2012

Précédentes versions de l'Avenant relatif au traitement des données pour les Services Looker (original) :

14 février 2023 4 janvier 2023 20 septembre 2022 30 juin 2022 16 mars 2022 24 septembre 2021 1er avril 2021 15 janvier 2021 17 décembre 2020 28 août 2020 1er juin 2020 9 mars 2020

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

6 février 2023 28 novembre 2022 27 septembre 2021 1er octobre 2020

Précédentes versions de l'Avenant relatif au traitement des données pour les Services de conseil SecOps et les Services gérés :

5 octobre 2023 19 septembre 2023 15 juin 2023 22 février 2023 6 février 2023

Versions précédentes *(Dernière modification le 15 octobre 2024)*

26 septembre 2024 9 septembre 2024 5 août 2024 23 mai 2024 9 avril 2024 8 novembre 2023 15 août 2023 20 septembre 2022