Cette traduction est fournie à des fins de commodité uniquement et pourrait ne pas refléter le sens du document original en anglais avec exactitude. Le sens des conditions et déclarations énoncées aux présentes est soumis à leurs définitions et interprétations en anglais. En cas de contradiction ou de conflit entre la version anglaise de ce texte et toute traduction, la version anglaise prévaudra.

AVENANT RELATIF AU TRAITEMENT DES DONNÉES DE CLOUDFLARE

Cloudflare, Inc. (« **Cloudflare** ») et le cocontractant convenant aux présentes (le « **Client** ») ont conclu un Contrat d'Abonnement d'Enterprise, un Contrat d'Abonnement en Libre-Service ou tout autre contrat écrit ou électronique relatif aux Services fournis par Cloudflare (l'« **Accord principal** »). Le présent Avenant relatif au traitement des données**,** et les annexes qui y sont jointes (collectivement, l'« **ATD** ») font partie intégrante de l'Accord principal.

Le présent ATD entrera en vigueur à la date à laquelle le Client signera ou à la date à laquelle les parties concluront autrement le présent ATD (la « **Date d'entrée en vigueur de l'ATD** ») ; il annulera et remplacera toutes les conditions antérieures applicables à l'objet des présentes (y compris toute modification, tout accord ou tout avenant relatif au traitement des données dans le cadre des Services).

Si vous acceptez le présent ATD pour le compte du Client, vous garantissez que : (a) vous êtes pleinement habilité par la loi à lier le Client par le présent ATD ; (b) vous avez lu et compris le présent ATD ; et (c) vous acceptez le présent ATD pour le compte du Client. Si vous n'êtes pas habilité à lier le Client, n'acceptez pas le présent ATD.

CONDITIONS RELATIVES AU TRAITEMENT DES DONNÉES

Le présent ATD s'applique lorsque Cloudflare traite des Données personnelles en tant que Sous-traitant (ou Sous-traitant ultérieur, selon le cas) pour le compte du Client et lorsque ces Données personnelles sont soumises aux Lois applicables en matière de protection des données (telles que définies ci-dessous).

Les parties sont convenues de conclure le présent ATD afin de garantir la mise en œuvre de protections appropriées pour lesdites Données personnelles comme l'exigent les Lois applicables en matière de protection des données. Par conséquent, Cloudflare s'engage à respecter les conditions suivantes eu égard à toutes les Données personnelles qu'elle traite en tant que Sous-traitant (ou Sous-traitant ultérieur, selon le cas) pour le compte du Client.

1. Définitions

1.1 Les définitions suivantes s'appliquent dans le présent ATD :

a) « **Pays adéquat** » s'entend d'un pays ou territoire reconnu en vertu des Lois européennes applicables en matière de protection des données comme offrant une protection adéquate pour les Données personnelles.

b) « **Société affiliée** » s'entend, en ce qui concerne une partie, de toute personne morale qui, directement ou indirectement, Contrôle, est Contrôlée par, ou est placée sous Contrôle commun avec cette partie (mais seulement tant que ce Contrôle existe).

c) « **Lois applicables en matière de protection des données** » s'entend de l'ensemble des lois et règlements qui s'appliquent au traitement des Données personnelles en vertu de l'Accord principal, y compris les Lois européennes applicables en matière de protection des données et les Lois des États-Unis en matière de protection des données.

d) « **Groupe Cloudflare** » s'entend de Cloudflare et de toutes ses Sociétés affiliées.

e) « **Contrôleur** » s'entend d'une entité qui détermine la fin et les moyens de traitement des données personnelles et comprend les termes Contrôleur, Entreprise ou autres termes analogues tels que définis dans le cadre des Lois applicables en matière de protection des données.

f) « **Groupe du Client** » désigne le Client et l'une quelconque de ses Sociétés affiliées.

g) « **CCT européennes** » désigne les clauses contractuelles types jointes à la Décision d'Exécution de la Commission Européenne numéro 2021/914 du 4 juin 2021 concernant les clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil.

h) « **Cadre de Protection des Données** » désigne le Cadre de Protection des Données de l'Union Européenne – États-Unis ("*EU-U.S. Data Privacy Framework*"), l'Extension Britannique du Cadre de Protection des Données de l'Union Européenne – États-Unis ("*UK Extension to the EU-U.S. Data Privacy Framework*"), et le Cadre de Protection des Données de la Suisse – États-Unis ("*Swiss-U.S. DPF*"), tels qu'ils sont définis par le Ministère du Commerce des États-Unis.

i) « **Lois européennes applicables en matière de protection des données** » s'entend de l'ensemble des lois et règlements de l'Union européenne, de l'Espace économique européen, de leurs États membres, de la Suisse et du Royaume-Uni, applicables au traitement des Données personnelles en vertu de l'Accord principal (y compris, si applicables, (i) le Règlement 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données personnelles et à la libre circulation de ces données (Règlement général sur la protection des données) (le « **RGPD européen** ») ; (ii) le RGPD européen transposé en droit anglais par l'article 3 de la loi sur le retrait de l'Union européenne (European Union (Withdrawal) Act) du Royaume-Uni de 2018 (le « **RGPD britannique** ») ; (iii) la Loi fédérale suisse sur la protection des données du 1 Septembre 2023 et ses ordonnances annexes (la "**LPD suisse**"), (iv) la directive sur la protection de la vie privée dans le secteur des communications électroniques (Directive 2002/58/CE) ; et toutes les lois nationales applicables en matière de protection des données promulguées en vertu des règlements et directives visés aux alinéas (i), (ii), (iii) et (iv), ou qui s'appliquent conjointement avec ces règlements et directives).

j) « **Données personnelles** » s'entend de toutes les données définies comme des « *données personnelles* », des « *informations personnelles* » ou des « *données à caractère personnel* » (ou terme similaire) en vertu des Lois applicables en matière de protection des données.

k) « **traitement** », « **personne concernée** » et « **autorité de contrôle** » s'entendent au sens donné à ces termes par les Lois européennes applicables en matière de protection des données.

l) « **Sous-traitant** » s'entend d'une entité qui traite des Données personnelles pour le compte du Responsable du traitement, y compris une entité à laquelle une autre entité divulgue les données personnelles d'une personne physique pour une finalité commerciale conformément à un contrat

écrit qui impose à l'entité recevant les informations de conserver, utiliser ou divulguer les Données personnelles uniquement aux fins de la fourniture des Services, et comprend les termes et expressions "fournisseur", fournisseur de services" ainsi que les autres termes analogues tels que définis dans les Lois applicables en matière de protection des données.

m) « **Services** » s'entend de l'ensemble des solutions basées sur le cloud proposées, commercialisées ou vendues par Cloudflare ou ses partenaires agréés et qui sont conçues pour améliorer les performances, la sécurité et la disponibilité des propriétés Internet, applications et réseaux, ainsi que tous logiciels, kits de développement logiciel et interfaces de programmation d'application (« **API** ») mis à disposition en connexion avec les solutions susmentionnées.

n) « **Transfert limité** » s'entend : (i) lorsque le RGPD européen ou la LPD suisse s'applique, d'un transfert de Données personnelles depuis l'Espace économique européen ou la Suisse (selon le cas) vers un pays situé en dehors de l'Espace économique européen ou autre que la Suisse (selon le cas) qui ne fait pas l'objet d'une décision d'adéquation de la Commission européenne ou du préposé fédéral suisse à la protection des données et à la transparence (selon le cas) ; et lorsque le RGPD britannique s'applique, d'un transfert de Données personnelles depuis le Royaume-Uni vers un autre pays, qui n'est pas basé sur les règles d'adéquation de l'article 17A de la loi britannique sur la protection des données de 2018 (Data Protection Act). Pour éviter toute ambiguïté, un transfert de Données personnelles vers les Etats-Unis en vertu du Cadre de Protection des Données n'est pas un Transfert limité.

o) « **Avenant du Royaume-Uni** » désigne l'Avenant sur le traitement international des données (Version B1.0) publié par l'Information Commissioner's Office dans le cadre de l'article s.119(a) de la loi britannique sur la protection des données de 2018, telle que mise à jour ou modifiée de temps à autre.

p) « **Lois des États-Unis en matière de protection des données** » s'entend de l'ensemble des lois et règlements des États-Unis d'Amérique applicables au traitement des données personnelles dans le cadre de l'Accord principal, et comprenant (a) la loi 'California Consumer Privacy Act' de 2018, telle que modifiée par la loi 'California Privacy Rights Act' de 2020 (Code civil californien, articles 1798.100 - 1798.199, 2022) ainsi que ses décrets d'application (collectivement, la « **CCPA** »), (b) la loi de l'État de Virginie 'Consumer Data Protection Act', si applicable, (c) la loi de l'État du Colorado 'Privacy Act' ainsi que ses décrets d'application, si applicable, (d) la loi de l'État de l'Utah 'Consumer Privacy Act', si applicable et (e) la loi de l'Etat du Connecticut SB6 concernant la confidentialité des données et le contrôle des activités en ligne, si applicable.

1.2 Une entité « **Contrôle** » une autre entité si elle : (a) détient la majorité des droits de vote dans cette entité ; (b) est un membre ou un actionnaire de cette entité et a le droit de destituer une majorité des membres de son conseil d'administration ou d'un organe de gestion équivalent ; (c) est membre ou actionnaire de cette entité et contrôle seule ou en vertu d'un accord avec d'autres actionnaires ou membres, la majorité des droits de vote dans cette entité ; ou (d) a le droit d'exercer une influence dominante sur cette entité conformément à ses documents constitutifs ou en vertu d'un contrat ; et deux entités sont traitées comme étant sous « **Contrôle commun** » si l'une d'entre elles contrôle l'autre (directement ou indirectement), ou si les deux sont contrôlées (directement ou indirectement) par la même entité.

1.3 Aux fins du présent ATD, le terme « Fournir » concernant les Services désigne la prestation des Services tels que définis dans l'Accord principal.

2. Statut des parties

2.1 Le type de Données personnelles traitées conformément au présent ATD et l'objet, la durée, la nature et la finalité du traitement, ainsi que les catégories de personnes concernées, sont décrits à l'Annexe 1.

2.2 Chaque partie garantit qu'elle respectera les Lois applicables en matière de protection des données en ce qui concerne les Données personnelles et qu'elle fournira le même niveau de confidentialité que celui requis dans ces dernières. Dans le cadre de la relation entre les parties, le Client est seul responsable de l'exactitude, de la qualité et de la licéité des Données personnelles et des moyens par lesquels le Client a acquis les Données personnelles.

2.3 En ce qui concerne les droits et obligations des parties en vertu du présent ATD concernant les Données personnelles, les parties reconnaissent et conviennent que le Client est le Responsable du traitement (ou un Sous-traitant traitant des Données personnelles pour le compte d'un Responsable du traitement tiers), et que Cloudflare est un Sous-traitant (ou un Sous-traitant ultérieur, selon le cas).

2.4 Si le Client est un Sous-traitant, le Client garantit à Cloudflare que les instructions et les actions du Client concernant les Données personnelles, y compris sa nomination de Cloudflare en tant qu'autre Sous-traitant et, le cas échéant, la conclusion des CCT européennes (telles que possiblement modifiées dans l'article 6.2 ci-après), ont été (et continueront d'être, pendant la durée du présent ATD) autorisées par le Responsable du traitement tiers concerné.

3. Obligations de Cloudflare

3.1 En ce qui concerne toutes les Données personnelles qu'elle traite dans son rôle de Sous-traitant des données ou de Sous-traitant ultérieur, Cloudflare garantit qu'elle :

(a) se contentera de ne traiter les Données personnelles que dans le cadre de l'objectif commercial limité et spécifié et fournira les Services et conformément : (i) aux instructions écrites du Client telles que définies dans le Contrat principal et le présent DPA, à moins que la législation applicable de l'Union ou d'un État membre à laquelle Cloudflare est soumis ne l'exige, et (ii) aux exigences des Lois sur la protection des données applicables. Dans le cas où Cloudflare est tenu de traiter des Données personnelles en vertu des Lois applicables sur la protection des données, Cloudflare informera le Client de cette exigence légale avant le traitement, à moins que cette loi n'interdise une telle information pour des raisons importantes d'intérêt public ;

(b) n'utilisera pas les Données personnelles à des fins de marketing ou de publicité ;

(c) mettra en œuvre des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié compte tenu des risques que présente le traitement des Données personnelles, notamment en prévenant toute destruction accidentelle ou illicite, perte, altération, divulgation non autorisée ou accès non autorisé aux Données personnelles. Ces mesures comprennent, sans limitation, les mesures de sécurité énoncées à l'Annexe 2 (« **Mesures de sécurité** »). Le Client reconnaît que les Mesures de sécurité évoluent avec les progrès et développements techniques et que Cloudflare est susceptible de mettre à jour ou modifier les Mesures de sécurité à tout moment, pour autant que ces mises à jour et modifications ne dégradent pas ni ne diminuent la sécurité globale du Service ;

(d) s'assurera que seul le personnel autorisé a accès à ces Données personnelles et que toute personne qu'elle autorise à avoir accès aux Données personnelles est soumise à des obligations contractuelles ou légales de confidentialité ;

(e) informera le Client dans les meilleurs délais dès qu'elle prend connaissance de toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données, aux fins de la fourniture des Services au Client par Cloudflare, ses Sous-traitants ultérieurs, ou tout autre tiers identifié ou non identifié (une « **Violation de données personnelles** ») et apportera au Client la coopération et l'assistance nécessaires en lien avec cette Violation de données personnelles, y compris en

fournissant toutes les informations utiles en la possession de Cloudflare concernant cette Violation de données personnelles dans la mesure où elle affecte les Données personnelles ;

(f) ne fera aucune annonce publique concernant une Violation de données personnelles (un « **Avis de violation** ») sans l'accord écrit préalable du Client, sauf si le droit applicable l'impose ;

(g) si Cloudflare est en mesure de vérifier qu'une Personne concernée est associée au Client, Cloudflare informera rapidement le Client si elle reçoit une requête d'une Personne concernée exerçant ses droits à la protection de ses données (y compris ses droits d'accès, de rectification ou à l'effacement) à l'égard de ses Données personnelles (une « **Requête d'une Personne concernée** »). Cloudflare ne répondra pas à une Requête d'une Personne concernée sans l'accord écrit préalable du Client, sauf pour confirmer que cette requête concerne le Client, ce à quoi le Client consent par les présentes ;

(h) si Cloudflare est en mesure de le faire, et conformément au droit applicable, elle apportera son assistance raisonnable au Client pour répondre à une Demande d'une Personne concernée exerçant ses droits à la protection de ses données (y compris ses droits d'accès, de rectification ou à l'effacement) à l'égard de ses Données personnelles, dans ce cas où le Client ne serait pas en mesure de répondre à une Demande d'une Personne concernée sans l'assistance de Cloudflare. Il appartient au Client de vérifier que le demandeur est la Personne concernée dont les Données personnelles font l'objet de la demande. Cloudflare décline toute responsabilité pour les informations fournies en toute bonne foi au Client en vertu du présent alinéa. Le Client prendra en charge tous les frais engagés par Cloudflare en lien avec la fourniture de cette assistance ;

(i) sauf disposition contraire du droit applicable, après la résiliation ou l'expiration de l'Accord principal ou l'achèvement du Service, au choix du Client, Cloudflare supprimera ou restituera toutes les Données personnelles (y compris les copies de celles-ci) traitées conformément au présent ATD ;

(j) en tenant compte de la nature du traitement et des informations dont dispose Cloudflare, Cloudflare fournira au Client l'assistance raisonnablement demandée par celui-ci dans le cadre des obligations de Cloudflare en vertu des Lois applicables en matière de protection des données en ce qui concerne :

  (i) les analyses d'impact relatives à la protection des données (au sens donné à ce terme dans les Lois applicables en matière de protection des données) ;

  (ii) les notifications à l'autorité de contrôle en vertu des Lois applicables en matière de protection des données et/ou les communications aux Personnes concernées par le Client en réponse à toute Violation de données personnelles ; et

  (iii) le respect par le Client de ses obligations en vertu des Lois applicables en matière de protection des données en ce qui concerne la sécurité du traitement ;

étant entendu que tous les frais engagés par Cloudflare en lien avec la fourniture de cette assistance seront à la charge du Client ; et

(k) informer le Client si, de l'avis de Cloudflare, toute instruction fournie par le Client en vertu de la clause 3.1(a) enfreint les Lois Applicables sur la Protection des Données, ou si Cloudflare détermine autrement qu'il ne peut plus remplir ses obligations en vertu des Lois applicables en matière de protection des données.

3.2 Dans la mesure où Cloudflare traite des Données personnelles pour le compte du Client dans le cadre de la CCPA, Cloudflare prend les engagements supplémentaires suivants envers le Client : Cloudflare ne conservera pas, n'utilisera pas et ne divulguera pas ces Données personnelles à d'autres fins que celles énoncées dans l'Accord Principal et le présent ATD et comme autorisé par le CCPA, y compris en vertu de toute exemption relative à une « vente ». Cloudflare ne « vendra » ni ne « partagera » ces Données personnelles, comme ces termes sont définis dans la CCPA. La présente clause 3.2 ne limite ni ne réduit les engagements de protection des données que Cloudflare prend envers le Client dans l'Accord principal ou le présent ATD.

3.3 Cloudflare certifie comprendre et s'engage à respecter les obligations et restrictions des clauses 2 et 3, ainsi que les Lois applicables en matière de protection des données.

4. Sous-traitance ultérieure

4.1 Cloudflare ne divulguera les Données personnelles aux Sous-traitants que dans le but spécifique de fournir les Services.

4.2 Cloudflare veillera à ce que tout Sous-traitant ultérieur qu'elle engage pour assurer un quelconque aspect du Service pour son compte en relation avec le présent ATD le fasse uniquement sur la base d'un contrat écrit qui impose à ce Sous-traitant ultérieur des conditions (c.-à-d. des obligations de protection des données) au moins aussi protectrices pour les Données personnelles que celles imposées à Cloudflare par le présent ATD (les « **Conditions applicables** »). Cloudflare veillera au respect des Conditions applicables par ce Sous-traitant ultérieur et sera responsable envers le Client de toute violation par ce Sous-traitant ultérieur de l'une quelconque des Conditions applicables.

4.3 Le Client accorde une autorisation écrite générale : (a) à Cloudflare pour nommer d'autres membres du Groupe Cloudflare en tant que Sous-traitants ultérieurs, et (b) à Cloudflare et aux autres membres du Groupe Cloudflare pour nommer des opérateurs de data centers tiers, et des prestataires de services commerciaux, techniques et de support client en tant que Sous-traitants ultérieurs pour soutenir la fourniture du Service.

4.4 Cloudflare maintient une liste des Sous-traitants ultérieurs disponible sur https://www.cloudflare.com/gdpr/subprocessors/ et ajoutera les noms des nouveaux Sous-traitants ultérieurs et des Sous-traitants ultérieurs remplaçants à la liste au moins trente (30) jours avant la date à laquelle ces Sous-traitants ultérieurs commenceront le traitement des Données personnelles. Si le Client s'oppose à tout nouveau Sous-traitant ultérieur ou tout Sous-traitant ultérieur remplaçant pour des raisons légitimes liées à la protection des données, il doit notifier cette opposition par écrit à Cloudflare dans les dix (10) jours suivant la notification, et les parties s'efforceront de résoudre le problème en toute bonne foi. Si Cloudflare peut raisonnablement fournir le Service au Client conformément à l'Accord principal sans utiliser les services du Sous-traitant ultérieur et décide de le faire à son entière discrétion, alors le Client n'aura aucun droit en vertu du présent article 4.3 concernant l'utilisation envisagée des services du Sous-traitant ultérieur. Si Cloudflare estime avoir besoin des services du Sous-traitant ultérieur et ne peut accepter l'opposition du Client à ce nouveau Sous-traitant ultérieur ou Sous-traitant ultérieur remplaçant, le Client peut résilier le Bon de commande avec prise d'effet à la date à laquelle Cloudflare commence à utiliser les services de ce nouveau Sous-traitant ultérieur ou Sous-traitant ultérieur remplaçant uniquement pour le ou les Services pour lesquels le nouveau Sous-traitant ultérieur traitera des Données personnelles. Si le Client ne s'oppose pas à tout sous-traitant ultérieur nouveau ou de remplacement dans les délais prévus par le présent article 4.3, le Client est réputé accepter le sous-traitant ultérieur et renoncer à son droit d'opposition.

5. Audit et dossiers

5.1 Conformément aux Lois applicables en matière de protection des données, Cloudflare mettra à la disposition du Client les informations en sa possession ou sous son contrôle que le Client pourrait

raisonnablement demander en vue de démontrer le respect par Cloudflare des obligations des Sous-traitants en vertu des Lois applicables en matière de protection des données en ce qui concerne son traitement des Données personnelles.

5.2 Cloudflare peut respecter le droit d'audit du Client en vertu des Lois applicables en matière de protection des données personnelles, en fournissant :

(a) un rapport d'audit ne datant pas de plus de treize (13) mois, préparé par un auditeur externe indépendant démontrant que les mesures techniques et organisationnelles de Cloudflare sont suffisantes et conformes aux normes d'audit reconnues dans l'industrie ;

(b) des informations supplémentaires que Cloudflare a en possession ou sous son contrôle à une autorité de contrôle en charge de la protection des données s'il demande des informations supplémentaires ou a besoin d'informations supplémentaires en relation avec le traitement des Données personnelles effectué par Cloudflare en vertu du présent ATD ; et

(c) si les Données personnelles du Client sont couvertes par des CCT européennes et que les informations mises à disposition en vertu du présent article 5.2 sont jugées insuffisantes par le Client, Cloudflare permettra au Client de demander un audit sur place par an au cours de la Durée (telle que définie dans l'Accord principal) afin de vérifier le respect par Cloudflare de ses obligations au titre du présent ATD ou des Lois applicables en matière de protection des données, conformément à l'article 5.3.

5.3 Les conditions supplémentaires suivantes s'appliquent aux audits demandés par le Client :

(a) Le Client doit faire parvenir toute demande de révision des rapports d'audit de Cloudflare à l'adresse customer-compliance@cloudflare.com

(b) Suite à la réception par Cloudflare d'une demande d'audit visée à l'alinéa 5.2(c), Cloudflare et le Client définiront d'un commun accord la date de début raisonnable, la portée et la durée de l'audit ainsi que les contrôles de sécurité et de confidentialité applicables à tout audit visé à l'alinéa 5.2(c). Si possible, les preuves d'audit se limiteront aux éléments probants recueillis lors du dernier audit tiers de Cloudflare.

(c) Cloudflare peut facturer des frais (basés sur les coûts raisonnables de Cloudflare) pour tout audit visés à l'alinéa 5.2(c). Cloudflare informera le Client des éventuels frais applicables, ainsi que de la base de calcul de ses frais, avant tout audit. Les frais facturés par tout auditeur mandaté par le Client pour réaliser un audit sont à la charge du Client.

(d) Cloudflare peut s'opposer par écrit à un auditeur mandaté par le Client pour réaliser un audit visé à l'alinéa 5.2(c) si Cloudflare estime raisonnablement que l'auditeur n'est pas suffisamment compétent ou indépendant, qu'il est un concurrent de Cloudflare ou qu'il est manifestement inapproprié pour toute autre raison (c.-à-d. que l'engagement de cet auditeur pourrait avoir un impact tout aussi préjudiciable sur les affaires de Cloudflare que les aspects susmentionnés). En cas d'opposition de Cloudflare, le Client doit mandater un autre auditeur ou réaliser l'audit lui-même. Si les CCT européennes (telles qu'elles peuvent être modifiées dans l'article 6.2 ci-après) s'appliquent, aucune stipulation du présent article 5.6 ne modifie les CCT européennes ni n'affecte les droits de toute autorité de contrôle ou personne concernée en vertu des CCT européennes.

6. Transferts de données depuis l'EEE, la Suisse et le Royaume-Uni

6.1 Dans le cadre du Service, les parties prévoient que Cloudflare (et ses Sous-traitants ultérieurs) puisse traiter, en dehors de l'Espace économique européen (« **EEE** »), de la Suisse et du Royaume-Uni, certaines Données personnelles protégées par les Lois européennes applicables en matière de protection

des données et dont le Client ou tout membre du Groupe du Client pourrait être le Responsable du traitement (ou le Sous-traitant d'un Responsable du traitement tiers, selon le cas).

6.2 Les parties conviennent que lorsque le transfert de Données personnelles protégé par les Lois européennes applicables en matière de protection des données, du Client ou de tout membre du Groupe du Client vers Cloudflare, est un Transfert limité, les clauses contractuelles types et les garanties supplémentaires appropriées s'appliquent comme suit :

(a) **Transferts au sein de l'UE.** Pour les Données personnelles protégées par le RGPD européen, les CCT européennes s'appliquent, complétées par ce qui suit :

(i) Le Module 2 s'applique lorsque le Client (ou le membre concerné du Groupe du Client) est un Responsable du traitement, et le Module 3 s'applique lorsque le Client (ou le membre concerné du Groupe du Client) est un Sous-traitant ;

(ii) à la clause 7, la clause d'adhésion facultative s'applique ;

(iii) à la clause 9, l'option 2 s'applique, et le délai de préavis de tout changement de Sous-traitant ultérieur est celui prévu à l'article 4.4 du présent ATD ;

(iv) à la clause 11, le paragraphe en option ne s'applique pas ;

(v) à la clause 17, l'option 2 s'applique et si le droit de l'État membre dans lequel l'exportateur de données est établi ne reconnaît pas de droits au tiers bénéficiaire, le droit allemand s'applique ;

(vi) à la clause 18(b), les litiges seront tranchés par les tribunaux de la juridiction compétente aux termes de l'Accord principal entre les parties ou, si cette juridiction n'est pas un État membre de l'UE, les tribunaux de Munich, en Allemagne. Dans tous les cas, la clause 17 et la clause 18(b) doivent être cohérentes : la juridiction compétente doit être dans le pays dont le droit s'applique ;

(vii) L'Annexe I des CCT européennes sont réputées complétées par les informations figurant à l'Annexe 1 au présent ATD ; et

(viii) L'Annexe II des CCT européennes sont réputées complétées par les informations figurant à l'Annexe 2 au présent ATD ;

(b) **Transferts depuis le Royaume-Uni** : concernant les Données personnelles protégées par le RGPD britannique, les CCT européennes, complétées comme le prévoit l'article 6.2(a) du présent ATD, s'appliquent aux transferts de ces Données personnelles, sauf dans les cas où :

(i) Les CCT européennes sont réputés modifiés comme spécifié par l'Avenant du Royaume-Uni, qui est réputé exécuté entre le Client cédant (ou le membre concerné du Groupe de Clients) et Cloudflare ;

(ii) Tout conflit entre les termes des CCT européennes et de l'Avenant du Royaume-Uni sera résolu conformément à la section 10 et à la section 11 de l'Avenant du Royaume-Uni;

(iii) Aux fins de l'Avenant du Royaume-Uni, les tableaux 1 à 3 de la partie 1 de l'Avenant du Royaume-Uni sont réputés remplis à l'aide des informations contenues dans les annexes du présent ATD ; et

(iv) Le tableau 4 de la partie 1 de l'Avenant du Royaume-Uni est réputé rempli en sélectionnant "aucune partie".

(c) **Transferts depuis la Suisse:** concernant les Données personnelles protégées par la LPD suisse (telles que modifiée ou remplacée), les CCT européennes, complétées comme le prévoit l'article 6.2(a) du présent ATD, s'appliquent aux transferts de ces Données personnelles, sauf que :

(i) l'autorité de contrôle compétente pour ces Données personnelles est le préposé fédéral suisse à la protection des données et à la transparence ;

(ii) dans l'article 17, le droit applicable est le droit suisse ;

(iii) les références aux « États membres » dans les CCT européennes doivent être interprétées comme des références à la Suisse, et les personnes concernées basées en Suisse sont en droit d'exercer et de faire valoir leurs droits en vertu des CCT européennes en Suisse ; et

(iv) les références au « Règlement général sur la protection des données », au « Règlement 2016/679 » ou au « RGPD » dans les CCT européennes doivent être comprises comme des références à la LPD suisse (telles que modifiée ou remplacée).

(d) Les termes suivants s'appliquent aux CCT européennes (en comprenant les éventuels amendements à ces derniers en vertu des articles 6.2(b)(ii) et 6.2(b)(iii) ci-avant) :

(i) Le Client peut exercer son droit d'audit en vertu des CCT européennes, comme précisé à l'article 5 du présent ATD et sous réserve des exigences énoncées à cet article ; et

(ii) Cloudflare peut nommer des Sous-traitants ultérieurs comme le prévoient les articles 4 et 6.3 du présent ATD, et sous réserve des exigences énoncées dans ces articles, et le Client peut exercer son droit d'opposition à des Sous-traitants ultérieurs en vertu des CCT européennes, comme le prévoit l'article 4.3 du présent ATD ; et

(e) En cas de contradiction directe ou indirecte entre une quelconque clause du présent ATD et les CCT européennes, les CCT européennes (ainsi que, le cas échéant, l'Avenant du Royaume-Uni) prévaudront.

6.3 En ce qui concerne les Transferts limités vers Cloudflare en vertu de l'article 6.2, Cloudflare s'interdit de participer (ou d'autoriser un quelconque Sous-traitant ultérieur à participer) à tout Transfert limité ultérieur de Données personnelles (que ce soit en tant qu'exportateur ou importateur des Données personnelles) à moins que ce Transfert limité ne soit effectué en totale conformité avec les Lois applicables en matière de protection des données et le cas échéant, toutes CCT européennes et/ou l'Avenant du Royaume-Uni mis en œuvre entre le Client et Cloudflare.

6.4 Le Client reconnaît que Cloudflare se conforme au Cadre de Protection des Données et que les transferts de Données du Client vers Cloudflare effectués en vertu du Cadre de Protection des Données ne constituent pas un Transfert limité. Cloudflare informera le Client si sa certification Cadre de Protection des Données expire ou est invalidée d'une autre manière, auquel cas tout transfert de Données personnelles du Client à Cloudflare sera immédiatement considéré comme un Transfert limité et les dispositions de l'article 6.2 ci-dessus s'appliqueront.

6.5 Si le Client souhaite effectuer une évaluation de l'adéquation des transferts de Cloudflare vers des pays ou des régions particuliers, Cloudflare devra, dans la limite de ses capacités, fournir une assistance

raisonnable au Client aux fins d'une telle évaluation, à condition que le Client couvre tous les frais encourus par Cloudflare pour fournir une telle assistance.

7. Demandes d'accès aux données de tiers

7.1 Si Cloudflare prend connaissance d'une procédure judiciaire intentée par un tiers demandant des Données personnelles que Cloudflare traite pour le compte du Client en sa qualité de Sous-traitant ou de Sous-traitant ultérieur (selon le cas), Cloudflare :

(a) informera immédiatement le Client de la demande, à moins que la loi interdise une telle notification ;

(b) informera le tiers qu'elle est un Sous-traitant ou un Sous-traitant ultérieur (selon le cas) des Données personnelles et qu'elle n'est pas autorisée à divulguer les Données personnelles sans l'accord du Client ;

(c) divulguera au tiers uniquement les coordonnées du Client strictement nécessaires pour permettre au tiers de contacter le Client et invitera le tiers à adresser sa demande au Client ; et

(d) si Cloudflare donne accès à des Données personnelles ou divulgue des Données personnelles dans le cadre d'une procédure judiciaire intentée par un tiers, soit avec l'autorisation du Client, soit en raison d'une obligation légale, Cloudflare divulguera le strict minimum nécessaire de Données personnelles.

7.2 En qualité de Sous-traitant ou de Sous-traitant ultérieur, selon le cas, Cloudflare peut faire l'objet d'une procédure judiciaire intentée par une autorité publique (y compris une autorité judiciaire) demandant l'accès à des Données personnelles ou la divulgation de Données personnelles. Si Cloudflare prend connaissance d'une procédure judiciaire intentée par une autorité publique (y compris une autorité judiciaire) demandant l'accès à des Données personnelles traitées par Cloudflare pour le compte du Client en qualité de Sous-traitant ou de Sous-traitant ultérieur (selon le cas), et que Cloudflare détermine que cette demande de Données personnelles crée un conflit d'intérêts, Cloudflare :

(a) prendra toutes les mesures énoncées à l'article 7.1 ci-dessus ;

(b) exercera un recours avant de produire les Données personnelles, jusque devant une juridiction d'appel ; et

(c) divulguera uniquement les Données personnelles requises en vertu des règles de procédure applicables.

7.3 Les articles 7.1 et 7.2 ne s'appliqueront pas si Cloudflare estime en toute bonne foi que la demande d'accès est légitime en raison d'une urgence mettant en danger la vie ou l'intégrité physique d'une personne. Dans ce cas, Cloudflare informera le Client de la divulgation des données dès que possible après la divulgation et fournira au Client toutes les informations concernant cette divulgation, à moins que cette divulgation ne soit interdite par la loi.

7.4 Cloudflare informera régulièrement le Client des procédures judiciaires intentées par des tiers demandant la fourniture de Données personnelles, sous la forme du Rapport de transparence semestriel de Cloudflare, disponible sur https://www.cloudflare.com/transparency/.

7.5 À la date de conclusion du présent ATD entre le Client et Cloudflare, Cloudflare prend les engagements énumérés ci-dessous. Cloudflare mettra à jour ces engagements au besoin sur https://www.cloudflare.com/transparency/:

(a) Cloudflare n'a jamais remis à quiconque ses clés de chiffrement ou d'authentification, ni celles de ses clients.

(b) Cloudflare n'a jamais installé d'outil logiciel ou d'équipement physique de surveillance en matière d'application de la loi sur son réseau.

(c) Cloudflare n'a jamais communiqué de flux relatif au contenu client transitant par notre réseau à un quelconque organisme chargé de l'application de la loi.

(d) Cloudflare n'a jamais affaibli, altéré ou détourné l'un de ses mécanismes de chiffrement à la demande des autorités ou d'un tiers.

8. Général

8.1 Le présent ATD est sans incidence sur les droits et obligations des parties en vertu de l'Accord principal, qui resteront en vigueur et de plein effet. En cas de conflit entre les clauses du présent ATD et les clauses de l'Accord principal, les clauses du présent ATD prévaudront dans la mesure où l'objet du conflit concerne le traitement de Données personnelles.

8.2 La responsabilité de Cloudflare en vertu du présent ATD ou en lien avec celui-ci, y compris en vertu des CCT européennes, est soumise aux exclusions et limitations de responsabilité énoncées dans l'Accord principal. Cloudflare ne limite ni n'exclut en aucun cas sa responsabilité envers les personnes concernées ou les autorités compétentes en charge de la protection des données.

8.3 À moins que les CCT européennes ne le prévoient expressément ou que les Lois applicables en matière de protection des données ne l'imposent, le présent ATD ne confère aucun droit de tiers bénéficiaire, et est destiné au seul bénéfice des parties aux présentes et de leurs successeurs et ayants droit autorisés respectifs. Aucun tiers au présent ATD ne peut faire valoir une quelconque clause des présentes.

8.4 Le présent ATD et toute action associée sont régis par le droit spécifié dans l'Accord principal, et doivent être interprétés conformément à ce droit, sans tenir compte de ses principes de conflit de lois. Les parties reconnaissent la compétence personnelle des tribunaux spécifiés dans l'Accord principal.

8.5 Si une quelconque clause du présent ATD était déclarée nulle ou inapplicable, pour quelque raison que ce soit, les autres clauses de l'ATD resteraient applicables. Sans limiter la généralité de ce qui précède, le Client convient que l'article 8.2 (Limitation de responsabilité) restera en vigueur nonobstant la nullité de toute disposition du présent ATD.

8.6 Le présent ATD constitue l'accord définitif, complet et exclusif des parties en ce qui concerne l'objet des présentes et remplace et regroupe toutes les discussions et tous les accords antérieurs entre les parties en ce qui concerne cet objet.

Annexe 1

Description du traitement des données

La présente Annexe 1 fait partie de l'ATD et décrit le traitement que Cloudflare effectuera pour le compte du Client.

A. LISTE DES PARTIES

Exportateur(s) de données : *Le Client remplit la colonne de droite.*

1.	Nom : *Le Client et les Sociétés affiliées du Client décrites dans l'Accord principal*	Comme indiqué dans l'Accord principal.
	Adresse : *Adresses du Client et des Sociétés affiliées du Client décrites dans l'Accord principal (ou autrement transmises par le Client à Cloudflare)*	Comme indiqué dans l'Accord principal
	Nom, fonction et coordonnées de la personne de contact :	Comme indiqué dans l'Accord principal
	Activités relatives aux données transférées dans le cadre du présent ATD et des CCT européennes :	Fourniture du Service au Client, conformément à l'Accord principal.
	Signature et date :	La présente Annexe 1 sera réputée signée à la signature de l'ATD.
	Rôle (Responsable du traitement/Sous-traitant) :	Responsable du traitement (ou Sous-traitant pour le compte d'un Responsable du traitement tiers).

Importateur(s) de données :

1.	Nom :	Cloudflare, Inc.
	Adresse :	101 Townsend Street San Francisco, CA 94107 É.-U.
	Nom, fonction et coordonnées de la personne de contact :	Emily Hancock Délégué à la protection des données legal@cloudflare.com

	Activités relatives aux données transférées dans le cadre du présent ATD et des CCT européennes :	Traitement nécessaire à la fourniture du Service au Client, conformément à l'Accord principal.
	Signature et date :	La présente Annexe 1 sera réputée signée à la signature de l'ATD.
	Rôle (Responsable du traitement/Sous-traitant) :	Sous-traitant (ou Sous-traitant ultérieur)

B. DESCRIPTION DU TRAITEMENT ET DU TRANSFERT DE DONNÉES

Catégories de personnes concernées dont les Données personnelles sont transférées :	Les personnes physiques qui (i) utilisent ou accèdent aux domaines, réseaux, sites web, interfaces de programmation d'applications (« API ») et applications du Client, ou (ii) les employés, agents ou sous-traitants du Client qui utilisent ou accèdent aux Services, tels que les utilisateurs finaux de Cloudflare Zero Trust (ensemble, les « Utilisateurs finaux »). Les personnes physiques détenant des identifiants de connexion pour un compte Cloudflare et/ou celles qui administrent l'un des Services pour un Client (les « Administrateurs »).
Catégories de Données personnelles transférées :	Concernant les Utilisateurs finaux : ● Toutes les Données personnelles traitées dans les Journaux du Client, telles que les adresses IP et, dans le cas de Cloudflare Zero Trust, les noms et adresses électroniques des utilisateurs finaux de Cloudflare Zero Trust. «Journaux du Client » s'entend de tous les journaux des interactions des Utilisateurs finaux avec les Propriétés Internet du Client et le Service qui sont mis à la disposition du Client via le tableau de bord du Service ou toute autre interface en ligne pendant la Durée par Cloudflare. ● Toute Donnée personnelle traitée dans le Contenu du Client, dont la teneur est déterminée et contrôlée par le Client à sa seule discrétion. « Contenu du Client » désigne tous les fichiers, logiciels, scripts, images multimédias, graphiques, contenu audio et vidéo, textes, données ou autres objets provenant de, ou transmis ou traités par toute Propriété Internet détenue, contrôlée ou exploitée par le Client ou transférés par le Client via le Service, et acheminés vers,

	transmis par, traités et/ou mis en cache sur ou dans le réseau de Cloudflare, ou transmis ou acheminés de toute autre manière à l'aide du Service par le Client. Concernant les Utilisateurs administratifs : ● Toute Donnée personnelle traitée les journaux d'audit de l'utilisateur administratif, comme les adresses IP ou adresses email.
Données sensibles transférées (le cas échéant) et restrictions ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, telles que la limitation stricte des finalités, les restrictions d'accès (notamment l'accès réservé au personnel ayant suivi une formation spécialisée), la tenue d'un registre d'accès aux données, les restrictions applicables aux transferts ultérieurs ou les mesures de sécurité supplémentaires :	Le Client, ses Utilisateurs finaux, Administrateurs et/ou autres partenaires peuvent déposer du contenu dans les propriétés en ligne du Client qui peuvent inclure des catégories particulières de données dont la teneur est déterminée et contrôlée par le Client à sa seule discrétion. Ces catégories particulières de données comprennent, entre autres, les informations révélant des origines raciales ou ethniques, des opinions politiques, des croyances religieuses ou philosophiques, l'appartenance syndicale et le traitement de données concernant la santé ou la vie sexuelle d'une personne. Ces catégories particulières de données sont protégées par l'application des mesures de sécurité décrites à l'Annexe 2.
Fréquence du transfert (par ex. si les données sont transférées sur une base ponctuelle ou continue) :	Continue pendant la durée de l'Accord principal.
Nature du traitement :	Traitement nécessaire à la fourniture du Service au Client, conformément aux instructions documentées de l'Accord principal et du présent ATD.
Finalité(s) du transfert et du traitement ultérieur des données :	Traitement nécessaire à la fourniture du Service au Client, conformément aux instructions documentées de l'Accord principal et du présent ATD.
Durée de conservation des Données personnelles ou, lorsque ce n'est pas possible, critères utilisés pour déterminer cette durée :	Jusqu'à la première occurrence entre (i) l'expiration/la résiliation de l'Accord principal, ou (ii) la date à laquelle le traitement n'est plus nécessaire aux fins de l'exécution par l'une ou l'autre des parties de ses obligations au titre de l'Accord principal (dans la mesure du possible).

Pour les transferts à des Sous-traitants (ultérieurs), veuillez également préciser l'objet, la nature et la durée du traitement :	L'objet, la nature et la durée du traitement seront spécifiés dans l'Accord principal.

C. AUTORITÉ DE CONTRÔLE COMPÉTENTE

Identifier la/les autorité(s) de contrôle compétente(s) (p.ex., conformément à l'article 13 des CCT européennes)	En ce qui concerne les CCT européennes, cela signifie l'autorité de contrôle compétente déterminée conformément à l'article 13 des CCT européennes. Concernant l'Avenant du Royaume-Uni, cela signifie le *UK Information Commissioner's Office*.

Annexe 2

Mesures de sécurité techniques et organisationnelles

Cloudflare a mis en place et maintiendra un programme de sécurité de l'information conforme aux normes ISO/IEC 27000. Le programme de sécurité de Cloudflare comprend :

Mesures de chiffrement des Données personnelles

Cloudflare utilise le chiffrement pour protéger correctement les Données personnelles à l'aide de :

- protocoles de chiffrement de pointe destinés à protéger efficacement contre les attaques actives et passives avec des ressources connues pour être accessibles aux autorités publiques;
- autorités et infrastructure de confiance pour la certification de clés publiques;
- algorithmes de chiffrement et paramétrage efficaces, comme une longueur de clé de 128 bits minimum pour le chiffrement symétrique, et un chiffrement RSA de 2048 bits ou ECC de 256 bits minimum pour les algorithmes asymétriques.

Mesures visant à garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement

Cloudflare renforce la sécurité des systèmes et services de traitement dans les environnements de production :

- en appliquant un processus d'examen des codes pour renforcer la sécurité du code utilisé pour fournir les Services, et en testant le code et les systèmes pour détecter les vulnérabilités avant et pendant l'utilisation ;
- en mettant en œuvre un programme de primes aux bogues externe ;
- en effectuant des vérifications pour valider l'intégrité des données chiffrées ; et
- en utilisant la détection préventive et réactive des intrusions.

Cloudflare déploie des systèmes à haute disponibilité dans des centres de données dispersés géographiquement.

Cloudflare met en œuvre des mesures de contrôle pour protéger la confidentialité des Données personnelles, y compris :

- une politique d'autorisation pour la saisie, la lecture, la modification et la suppression des données ;
- l'authentification du personnel autorisé à l'aide d'identifiants d'authentification unique (mots de passe) et de jetons de sécurité physiques ;
- la déconnexion automatique des utilisateurs après une période d'inactivité ;
- la protection de la saisie de données, ainsi que contre la lecture, la modification et la suppression des données stockées ; et
- l'obligation de maintenir les installations de traitement des données (les salles hébergeant le matériel informatique et l'équipement associé) fermées à clé et sécurisées.

Mesures garantissant de disposer de moyens permettant de rétablir la disponibilité des données personnelles et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique

Cloudflare met en œuvre des mesures garantissant la protection des Données personnelles contre toute destruction ou perte accidentelle, notamment :

- des plans et procédures de reprise après sinistre et de continuité des activités ;
- des centres de données dispersés géographiquement ;
- des infrastructures redondantes, y compris l'alimentation en électricité et la connexion Internet ;
- des sauvegardes stockées sur des sites alternatifs et disponibles pour la restauration en cas de défaillance des systèmes principaux ; et

- des procédures de gestion des incidents testées régulièrement.

Procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles afin de garantir la sécurité du traitement

Les mesures techniques et organisationnelles de Cloudflare sont testées et évaluées régulièrement par des auditeurs tiers externes dans le cadre du Programme de Conformité Sécurité et Confidentialité de Cloudflare. Cela inclut des audits annuels ISO/IEC 27001, des audits AICPA SOC 2 Type II, PCI DSS niveau 1 et d'autres audits externes. En outre, les mesures sont régulièrement testées par des audits internes ainsi que par des évaluations des risques annuelles et ciblées.

Mesures d'identification et d'autorisation de l'utilisateur

Cloudflare met en œuvre des mesures efficaces pour l'authentification des utilisateurs et la gestion des droits d'accès, notamment :

- une politique de contrôle d'accès et d'authentification obligatoires ;
- un modèle d'identification et d'autorisation zéro Trust ;
- l'authentification du personnel autorisé à l'aide d'identifiants d'authentification unique et de l'authentification forte multi-facteurs, y compris l'utilisation obligatoire de jetons de sécurité physique ;
- l'attribution et la gestion des droits d'accès appropriés en fonction du rôle, des autorisations, et la gestion des exceptions ; et
- l'application du principe de moindre privilège.

Mesures de protection des données pendant la transmission

Cloudflare met en œuvre des mesures efficaces pour empêcher que les Données personnelles ne soient lues, copiées, modifiées ou supprimées par des parties non autorisées pendant leur transmission, notamment :

- des protocoles de chiffrement de pointe destinés à protéger efficacement contre les attaques actives et passives avec des ressources connues pour être accessibles aux autorités publiques ;
- des autorités et infrastructure de confiance pour la certification de clés publiques ;
- l'utilisation de mesures de protection contre les attaques actives et passives ciblant les systèmes émetteurs et récepteurs assurant le chiffrement pendant la transmission, comme des pare-feux appropriés, le chiffrement TLS mutuel, l'authentification API et le chiffrement pour protéger les passerelles et les pipelines par lesquels les données transitent, ainsi que des tests visant à détecter les vulnérabilités des logiciels et les portes dérobées potentielles ;
- l'utilisation d'algorithmes de chiffrement et un paramétrage efficaces, comme une longueur de clé de 128 bits minimum pour le chiffrement symétrique, et un chiffrement RSA de 2048 bits ou ECC de 256 bits minimum pour les algorithmes asymétriques ;
- des logiciels correctement implémentés et tenus à jour, couverts par un programme de gestion des vulnérabilités et dont la conformité est testée par des audits ;
- l'application de mesures de sécurité pour générer, gérer, stocker et protéger de manière fiable les clés de chiffrement ; et
- journaux d'audits, surveillance et suivi des transmissions de données.

Mesures de protection des données pendant le stockage

Cloudflare met en œuvre des mesures efficaces pour protéger les Données personnelles pendant le stockage, en contrôlant et en limitant l'accès aux systèmes de traitement des données, et au moyen de :

- protocoles de chiffrement de pointe destinés à protéger efficacement contre les attaques actives et passives avec des ressources connues pour être accessibles aux autorités publiques ;
- des autorités et infrastructure de confiance pour la certification de clés publiques ;

- la réalisation de tests des systèmes de stockage de données visant à détecter les vulnérabilités des logiciels et les portes dérobées potentielles ;
- algorithmes de chiffrement et paramétrage efficaces, comme l'obligation de chiffrer tous les disques stockant des Données personnelles avec AES-XTS en utilisant une longueur de clé de 128 bits minimum.
- des logiciels correctement implémentés et tenus à jour, couverts par un programme de gestion des vulnérabilités et dont la conformité est testée par des audits ;
- mesures de sécurité pour générer, gérer, stocker et protéger de manière fiable les clés de chiffrement ;
- l'identification et l'autorisation des systèmes et utilisateurs ayant accès à des systèmes de traitement de données ;
- la déconnexion automatique des utilisateurs après une période d'inactivité ; et
- journaux d'audits, surveillance et suivi de l'accès aux systèmes de traitement et de stockage de données.

Cloudflare met en œuvre des contrôles d'accès pour des zones spécifiques des systèmes de traitement des données, afin de garantir que seuls les utilisateurs autorisés puissent accéder aux Données personnelles relevant du champ d'application de leurs droits d'accès et que les Données personnelles ne puissent pas être lues, copiées, modifiées ou supprimées sans autorisation. À cette fin, diverses mesures seront mises en œuvre, notamment :

- politiques applicables au personnel et formation du personnel sur leurs droits d'accès spécifiques aux Données personnelles ;
- un modèle d'identification et d'autorisation zéro Trust ;
- l'authentification du personnel autorisé à l'aide d'identifiants d'authentification unique et de l'authentification forte multi-facteurs, y compris l'utilisation obligatoire de jetons de sécurité physique ;
- la surveillance des actions des personnes autorisées à supprimer, ajouter ou modifier des Données personnelles ;
- la divulgation de données uniquement aux personnes autorisées, y compris attribution de droits d'accès et de rôles différenciés ; et
- le contrôle d'accès aux données, avec une destruction contrôlée et documentée des données.

Mesures visant à garantir la sécurité physique des lieux où les Données personnelles sont traitées

Cloudflare met en œuvre des politiques et mesures de contrôle d'accès physique efficaces afin d'empêcher des personnes non autorisées d'accéder à l'équipement de traitement des données (à savoir les serveurs de base de données et d'application et le matériel associé) sur lequel les Données personnelles sont traitées ou utilisées, y compris :

- en définissant des zones de sécurité ;
- en protégeant et en limitant les chemins d'accès ;
- en établissant des autorisations d'accès pour les employés et tiers, y compris la documentation associée ;
- en journalisant, en surveillant et en suivant tous les accès aux centres de données où les Données personnelles sont hébergées ; et
- en protégeant les centres de données où les Données personnelles sont hébergées par des systèmes d'alarme et d'autres mesures de sécurité appropriées.

Mesures visant à garantir la journalisation des événements

Cloudflare a mis en œuvre un programme de journalisation et de suivi pour journaliser, contrôler et suivre l'accès aux données personnelles, y compris par les administrateurs système, et pour garantir que les données sont traitées conformément aux instructions reçues. Ces mesures incluent notamment :

- l'authentification du personnel autorisé à l'aide d'identifiants d'authentification unique et de l'authentification forte multi-facteurs, y compris l'utilisation obligatoire de jetons de sécurité physique ;
- un modèle d'identification et d'autorisation zéro Trust ;
- la tenue à jour des listes d'identifiants des administrateurs système ;
- l'adoption de mesures visant à détecter les anomalies à haut risque, les analyser et y répondre ;
- la conservation de journaux sécurisés, précis et non altérés, répertoriant les accès à l'infrastructure de traitement, pendant douze mois ; et
- au moins une fois par an, un test de la configuration de la journalisation, du système de surveillance et du processus d'alerte et de réponse aux incidents.

Mesures visant à garantir la configuration du système, notamment la configuration par défaut

Cloudflare applique des bases de référence pour la configuration de tous les systèmes appuyant l'environnement de traitement des données de production, y compris les systèmes tiers. Les bases de référence de configuration doivent être alignées sur les bonnes pratiques de l'industrie telles que les références de niveau 1 du *Center for Internet Security* (CIS). Des mécanismes automatisés doivent être utilisés pour appliquer les configurations de référence aux systèmes de production et pour empêcher les modifications non autorisées. Les bases de référence peuvent être modifiées seulement par quelques membres du personnel autorisé de Cloudflare et en suivant les processus de contrôle des modifications. Les modifications doivent être vérifiables et vérifiées régulièrement pour détecter les écarts par rapport aux configurations de référence.

Cloudflare configure des bases de référence pour le système d'information en utilisant le principe de moindre privilège. Par défaut, les configurations d'accès sont définies sur « tout refuser » et les mots de passe par défaut doivent être modifiés pour respecter les politiques de Cloudflare avant l'installation de l'appareil sur le réseau Cloudflare, ou immédiatement après l'installation du logiciel ou du système d'exploitation. Les systèmes sont configurés pour synchroniser les horloges système avec le temps atomique international ou le temps universel coordonné (UTC), et l'accès pour modifier l'heure est limité au personnel autorisé.

Mesures pour la gouvernance et la gestion de l'informatique interne et de la sécurité informatique

Cloudflare applique des politiques internes relatives à l'utilisation acceptable des systèmes informatiques et à la sécurité de l'information en général. Cloudflare impose à tous ses employés de suivre une formation générale de sensibilisation à la sécurité et à la confidentialité au moins une fois par an. Cloudflare limite et protège le traitement des Données personnelles, et a documenté et mis en œuvre :

- un système de gestion de la sécurité de l'information (ISMS) formel, afin de protéger la confidentialité, l'intégrité, l'authenticité et la disponibilité des données et des systèmes d'information de Cloudflare, et assurer l'efficacité des contrôles de sécurité sur les données et les systèmes d'information qui appuient les opérations ; et
- un système de gestion des informations personnelles (PIMS) formel afin de protéger la confidentialité, l'intégrité, l'authenticité et la disponibilité des politiques et procédures soutenant le réseau mondial de Cloudflare, en tant que sous-traitant et responsable du traitement d'informations client.

Cloudflare conservera la documentation des mesures techniques et organisationnelles en cas de vérifications, et pour la conservation des preuves. Cloudflare prendra des mesures raisonnables pour s'assurer que les personnes qu'elle emploie, et d'autres personnes sur le lieu de travail concerné, connaissent les mesures techniques et organisationnelles énoncées dans la présente Annexe 2 et les respectent.

Mesures de certification/assurance des processus et des produits

La mise en œuvre de l'ISMS de Cloudflare et les processus de gestion des risques de sécurité associés ont été certifiés ISO/IEC 27001 par des organismes indépendants. La mise en œuvre du PIMS complet de Cloudflare a été certifiée ISO/IEC 27701 par un organisme indépendant, en tant que sous-traitant et responsable du traitement d'informations client.

Cloudflare conserve la certification PCI DSS de niveau 1, pour laquelle Cloudflare est auditée chaque année par un auditeur de sécurité qualifié tiers. Cloudflare a entrepris d'autres démarches de certification, notamment pour obtenir la certification AICPA SOC 2 Type II conformément au référentiel de critères de confiance (Trust Service Criteria) de l'AICPA, et des informations sur ces certifications et sur les autres démarches de certification que Cloudflare pourrait entreprendre à tout moment seront publiées sur le site Web de Cloudflare.

Pour les transferts vers des Sous-traitants (ultérieurs), veuillez également décrire les mesures techniques et organisationnelles que le Sous-traitant (ultérieur) doit prendre pour être en mesure d'aider le responsable du traitement (et, pour les transferts d'un Sous-traitant à un Sous-traitant ultérieur, l'exportateur de données).

Accès libre-service pour répondre aux droits d'accès, d'effacement, de rectification, etc. des personnes concernées.	Capacité de se connecter pour examiner et éditer les Données personnelles via le tableau de bord de Cloudflare.