ADDENDUM RELATIF À LA PROTECTION DES DONNÉES

Le présent addendum relatif à la protection des données (« APD » ou « addendum ») est partie intégrante du contrat de services conclu entre (« Planet ») et (le « commerçant ») en date du (le « contrat »).

Planet et le commerçant (chacun étant individuellement dénommé « partie » et conjointement « parties ») conviennent que le présent APD expose les exigences en matière de protection des données qui s'appliquent au traitement des données à caractère personnel (ou, le cas échéant, des données à caractère personnel partagées) par les parties aux fins énoncées dans le contrat et/ou le présent APD.

1. Définitions

Dans le présent addendum, il est fait application des définitions suivantes :

1.1. Entreprises liées : toutes personnes physiques ou morales, tous partenariats, associations ou entreprises qui, directement ou indirectement, par l'entremise d'un ou plusieurs intermédiaires, contrôlent une partie, sont contrôlés par elle ou sont sous contrôle commun avec une partie, selon le cas, ou leurs successeurs respectifs. Le terme « contrôle », y compris les termes « contrôler », « contrôlé(e) par » et « sous contrôle commun avec », désigne la détention, directe ou indirecte, du pouvoir de déterminer ou de faire déterminer l'orientation de la gestion et des politiques d'une société, d'un partenariat, d'une association ou d'une entreprise, que ce soit par la possession d'actions assorties du droit de vote, par contrat ou de toute autre manière. Les entreprises liées englobent toutes entités actuellement existantes ou créées ultérieurement par investissement, fusion ou de toute autre manière, y compris les successeurs et les ayants droit de ces entités.

1.2. Lois applicables : toutes lois, réglementations, décisions gouvernementales, dispositions, directives et modifications de celles-ci présentant une pertinence juridique au sein de la juridiction concernée, ainsi que toutes décisions prises par les entités gouvernementales compétentes, dans toutes juridictions pertinentes pour le contrat, y compris, mais sans y être circonscrites, les réglementations régissant la profession d'intermédiaire bancaire et tous codes monétaires et financiers applicables dans les pays concernés, la législation sur la lutte contre le blanchiment d'argent (LCB), de lutte contre le financement du terrorisme (LFT), les embargos, les sanctions, la corruption, les fautes professionnelles, les informations confidentielles (y compris la propriété intellectuelle et les secrets commerciaux), le comportement des institutions financières et la législation sur la protection des données.

1.3. Responsable du traitement des données : ce terme a le sens donné au terme « responsable » lorsqu'il détermine les finalités de toute donnée à caractère personnel et les moyens de son traitement, tels que définis dans la législation relative à la protection des données.

1.4. Sous-traitant : ce terme a la signification donnée au terme « sous-traitant » lorsque tout autre organisme traite des données à caractère personnel pour le compte d'un responsable du traitement des données, conformément à la législation sur la protection des données.

1.5. Législation sur la protection des données : le Règlement général sur la protection des données 2016/679 (RGPD), la nouvelle Loi fédérale suisse sur la protection des données (nLPD), le UK Data Protection Act de 2018, les UK Privacy and Electronic Communications Regulations de 2003, la Loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et toutes autres lois applicables relatives au traitement des données à caractère personnel, chacune dans leur version en vigueur.

1.6. Incident lié à la sécurité des données : désigne tout accès, traitement, toute suppression, perte ou toute forme de traitement illicite des données à caractère personnel (ou, le cas échéant, des données à caractère personnel partagées) non autorisé(e) ou accidentel(le) et/ou toute violation de la sécurité et/ou de la confidentialité entraînant, accidentellement ou de manière illicite, leur destruction, leur perte, leur altération, leur divulgation non autorisée ou l'accès aux données à caractère personnel (ou, le cas échéant, aux données à caractère personnel partagées).

1.7. Personne concernée : personne physique identifiée ou identifiable à laquelle se rapportent les données à caractère personnel.

1.8. **Demande d'une personne concernée :** désigne toute demande formelle faite par une personne concernée dans le but d'exercer ses droits, à savoir (i) d'accéder à ses données à caractère personnel ; (ii) de faire corriger ou effacer ses données à caractère personnel ; (iii) de limiter le traitement de ses données à caractère personnel ou de s'y opposer ; (iv) de demander la portabilité de ses données à caractère personnel ; (v) de ne pas faire l'objet d'une prise de décision automatisée (y compris le profilage) ou (vi) en relation avec tout autre droit que la personne concernée est habilitée à exercer dans toute juridiction pertinente à laquelle s'applique le présent APD.

1.9. **Données à caractères personnel :** toutes données à caractère personnel permettant d'identifier une personne physique (telles que définies dans la législation relative à la protection des données) traitées dans le cadre du contrat.

1.10. **Données à caractère personnel partagées :** toutes données à caractère personnel permettant d'identifier une personne physique (telles que définies dans la législation relative à la protection des données) traitées dans le cadre du contrat si les parties agissent en tant que responsables indépendants du traitement des données dans le contexte d'une « relation entre un responsable du traitement des données et un autre responsable du traitement des données ».

1.11. **Clauses contractuelles types :** désigne (i) les clauses contractuelles types pour transferts internationaux publiées par la Commission européenne le 4 juin 2021 et régissant le transfert de données à caractère personnel de l'EEE vers des pays tiers, telles qu'adoptées par la Commission Européenne (disponibles sur le site Internet de la Commission Européenne : https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en), et par le préposé fédéral à la protection des données et à la transparence (**« PFPDT »**) concernant les transferts de données vers des pays tiers (dénommées collectivement **« EU SCCs »**) ; (ii) l'addendum sur les transferts internationaux de données (**« UK Transfer addendum »**) adopté par le UK Information Commissioner's Office (**« UK ICO »**) pour les transferts de données du Royaume-Uni vers des pays tiers ; (iii) toutes clauses similaires (le cas échéant) adoptées par une autorité de contrôle de la protection des données relatives aux transferts de données vers des pays tiers ou (iv) toutes clauses succédant aux clauses (i) à (iii).

1.12. **Sous-traitant ultérieur :** désigne une entité mandatée par un sous-traitant pour traiter des données à caractère personnel pour le compte de ce sous-traitant.

1.13. **Autorité de contrôle :** désigne une autorité publique indépendante qui est soit (i) l'autorité mise en place par un État membre de l'UE conformément à l'article 51 du RGPD, soit (ii) l'autorité publique chargée de la protection des données investie d'un pouvoir de contrôle et d'une compétence juridictionnelle à votre égard.

2. Rôles en matière de protection des données

Dans le cadre de la fourniture des services offerts par Planet au commerçant en vertu du contrat, chacune des parties pourra, de temps à autre, fournir ou mettre à la disposition de l'autre partie des données à caractère personnel. Les parties conviennent qu'en fonction des prestations de service commandées, les rôles en matière de protection des données qui leur sont attribués aux fins de la législation sur la protection des données seront soit (i) responsables indépendants du traitement des données (dans le cadre d'une relation entre un responsable du traitement des données et un autre responsable du traitement des données), soit (ii) responsables du traitement des données (dans le cadre d'une relation entre un sous-traitant et un responsable du traitement des données), soit (iii) sous-traitants pour le compte de l'autre partie (dans le cadre d'une relation entre un sous-traitant et un responsable du traitement des données). Ceci ayant été préalablement exposé,

a) si les parties traitent des données à caractère personnel en qualité de responsables indépendants du traitement des données, il sera fait application du paragraphe 3 du présent APD.
b) Si une partie traite des données à caractère personnel en qualité de responsable du traitement, dans le cadre d'une relation entre un responsable du traitement des données et un sous-traitant, il sera fait application à cette partie du paragraphe 4 du présent APD.

c) Si une partie traite des données à caractère personnel en qualité de sous-traitant pour le compte de l'autre partie, il sera fait application à cette partie du paragraphe 5 du présent APD.

Une description complète des rôles et des finalités pour lesquels les données à caractère personnel (ou, le cas échéant, les données à caractère personnel partagées) seront traitées dans le cadre des services prévus par le contrat figure à l'Annexe 1.

3. Obligations applicables aux parties agissant en qualité de responsables indépendants du traitement des données

Le présent paragraphe 3 s'appliquera dans le cas où les parties agissent en tant que responsables indépendants du traitement des données.

3.1. Généralités

3.1.1. Les parties se communiqueront régulièrement les données à caractère personnel aux fins énoncées dans le contrat et/ou l'APD (**« données à caractère personnel partagées »**) et conviennent qu'en ce qui concerne ces données à caractère personnel partagées, chaque partie agira à part entière en tant que responsable du traitement et déterminera de manière indépendante les finalités et les moyens du traitement de ces données.

3.2. Traitement des données à caractère personnel partagées

3.2.1. Dès lors qu'une partie, dans le cadre de la prestation de services, agira en tant que responsable du traitement des données à caractère personnel partagées, elle sera tenue de respecter et d'exécuter ses obligations en vertu de la législation relative à la protection des données et devra notamment :

a) garantir que les données à caractère personnel partagées fournies ou mises à disposition dans le cadre du contrat sont exactes et actuelles ;
b) garantir qu'elle dispose d'une base juridique appropriée pour le traitement des données à caractère personnel partagées telle que décrite dans le présent APD et/ou dans le contrat ;
c) veiller à ce que toutes notifications nécessaires relatives au traitement équitable (communément dénommées « avis de confidentialité » ou « politiques de confidentialité ») soient fournies aux personnes concernées par le traitement des données lors de la collecte de leurs données à caractère personnel afin de permettre le traitement licite (y compris la collecte et le partage) des données à caractère personnel partagées aux fins énoncées dans le contrat et/ou l'APD ;
d) garantir que – sauf si une autre base juridique prévue par les lois sur la protection des données justifie la licéité du traitement – tout consentement nécessaire de la personne concernée au traitement sera obtenu et enregistré et, au cas où une personne concernée révoquerait son consentement, veiller à ce qu'il en soit fait communication à l'autre partie.

3.2.2. Chaque partie s'engage à ne pas fournir à l'autre partie des données à caractère personnel d'une catégorie spécifique (telles que des données relatives à la santé) non nécessaires à l'exécution des prestations de service.

3.3. Sécurité des données

3.3.1. Chaque partie prendra des mesures appropriées pour garantir la fiabilité des personnes susceptibles de traiter les données à caractère personnel partagées, notamment en veillant à ce que (i) l'accès soit strictement limité aux personnes qui ont besoin de connaître les données à caractère personnel partagées concernées ou d'y accéder aux fins décrites dans l'accord et/ou le présent APD et à ce que (ii) ces personnes soient soumises à des engagements de confidentialité ou à des obligations professionnelles ou légales de confidentialité.

3.3.2. Les parties mettront en œuvre et maintiendront des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (en tenant compte de la nature, de la portée, du contexte et des finalités du traitement), notamment contre tout traitement non autorisé ou illicite, ou toute perte, destruction ou détérioration accidentelle de ces données à caractère personnel partagées. En particulier, Planet appliquera

les mesures techniques et organisationnelles suivantes, disponibles à l'adresse https://www.weareplanet.com/technical-and-organisational-measures, dont un résumé figure à l'Annexe 2.

3.3.3. La partie recevant les données à caractère personnel partagées ne devra pas les conserver ou les traiter plus longtemps que nécessaire aux fins énoncées dans le contrat et/ou le présent APD et sera responsable de la mise en œuvre des mesures appropriées pour garantir que les données à caractère personnel partagées seront détruites ou supprimées lorsqu'elles ne seront plus nécessaires à ces fins. Nonobstant ce qui précède, chaque partie pourra continuer à conserver les données à caractère personnel partagées conformément aux délais de conservation légaux ou professionnels applicables.

3.4. Droits des personnes concernées

3.4.1. Chaque partie est responsable du traitement de ses propres demandes de personnes concernées relatives aux données à caractère personnel partagées et fournira l'assistance raisonnablement nécessaire pour permettre à l'autre partie de satisfaire aux demandes de ces personnes concernées.

3.4.2. Si une partie reçoit une demande de la personne concernée relative aux données à caractère personnel partagées qui concerne un traitement pour lequel l'autre partie est le responsable du traitement, la partie qui reçoit cette demande de la personne concernée devra la transmettre sans délai à l'autre partie. Sur demande écrite raisonnable, la partie qui reçoit la demande de la personne concernée devra fournir une coopération et une assistance appropriées afin de permettre à l'autre partie de satisfaire cette demande en respectant les délais applicables prévus par la législation sur la protection des données.

3.5. Incidents liés à la sécurité des données

3.5.1. Lorsqu'une partie aura connaissance d'un incident lié à la sécurité des données ayant une incidence significative sur le traitement des données à caractère personnel partagées, elle en informera sans délai l'autre partie et coopérera avec elle afin de lui permettre de mener une enquête sur l'incident, de formuler une réponse appropriée et de prendre les mesures adéquates supplémentaires en ce qui concerne l'incident lié à la sécurité des données.

3.5.2. En cas de survenance d'un incident lié à la sécurité des données concernant les données à caractère personnel partagées, ou s'il y a lieu de soupçonner qu'un incident lié à la sécurité des données s'est produit ou pourrait se produire, chaque partie en informera l'autre partie par écrit dans les plus brefs délais, en lui fournissant toutes informations pertinentes concernant les détails de l'incident, afin de permettre à cette partie de satisfaire à la législation sur la protection des données. Les informations pertinentes relatives à l'incident lié à la sécurité des données comprendront :

a) le nom, le nom commercial et les informations censées avoir été impactées ;
b) une description de la nature de l'incident, y compris, si possible, les catégories et le nombre approximatif de personnes concernées ;
c) le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact où des informations complémentaires pourront être obtenues ;
d) une description des conséquences probables de l'incident ;
e) une description des mesures prises ou proposées pour y remédier, y compris, le cas échéant, les mesures visant à atténuer ses éventuelles incidences négatives
f) et une copie de toute la correspondance s'y rapportant, y compris toute correspondance avec toutes personnes concernées.

3.6. Assistance mutuelle

3.6.1. Sur demande raisonnable, chaque partie devra fournir à l'autre partie une assistance, des informations et une coopération appropriées afin de garantir le respect de leurs obligations respectives en vertu de la législation sur la protection des données.

3.6.2. Si une partie reçoit une plainte, un avis ou une communication d'une autorité de contrôle qui concerne directement le traitement, par l'autre partie, des données à caractère personnel partagées ou un éventuel manquement de cette partie à la législation sur la protection des données en rapport avec les services fournis, la partie qui reçoit la plainte, l'avis ou la communication devra, dans la mesure où la législation applicable le permet, en informer rapidement l'autre partie et lui fournir les informations qu'elle peut raisonnablement demander à ce sujet.

3.7. Transferts internationaux de données

3.7.1. Les parties ne pourront traiter les données à caractère personnel partagées qu'au sein de l'EEE, du Royaume-Uni ou de la Suisse (selon le cas) ou dans d'autres pays reconnus par la Commission Européenne, le UK Information Commissioner's Office (ICO) ou le PFPDT suisse (selon le cas) comme garants d'un niveau adéquat de protection des données à caractère personnel en ce qui concerne la confidentialité des données et les droits et libertés fondamentaux des personnes.

3.7.2. Lorsqu'une partie transférera ou exportera des données à caractère personnel partagées vers un pays tiers situé hors de l'EEE, du Royaume-Uni ou de la Suisse (selon le cas) dépourvu d'un niveau de protection adéquat tel que déclaré par la Commission Européenne, l'ICO ou le PFPDT suisse (selon le cas), elle devra satisfaire à ses obligations en vertu de la législation sur la protection des données (i) en faisant usage de tous mécanismes appropriés de contrôle des transferts reconnus comme garantie adéquate par la législation sur la protection des données ou (ii) en soumettant les conditions de ce transfert aux clauses contractuelles types qui seront intégrées au présent contrat.

3.7.3. En outre, la partie transférant ou exportant les données à caractère personnel partagées devra mettre en œuvre et intégrer au présent APD toutes mesures supplémentaires adéquates qui soient pertinentes en fonction du risque réglementaire du pays de destination, garantissant ainsi un niveau de protection des données équivalent, pour l'essentiel, au niveau de protection en vigueur dans l'EEE, au Royaume-Uni ou en Suisse, selon le cas.

3.7.4. Dans la mesure où la partie transférant ou exportant les données à caractère personnel partagées s'appuie sur un mécanisme légal spécifique pour normaliser les transferts internationaux de données et que ce mécanisme est ensuite modifié, révoqué ou invalidé par un Tribunal compétent, les parties conviennent de coopérer en toute bonne foi afin de trouver un autre mécanisme approprié pouvant légalement soutenir le transfert.

4. Obligations applicables à une partie agissant comme responsable du traitement des données

Le présent paragraphe 4 s'applique dans le cas où une partie agit en tant que responsable du traitement des données dans le cadre d'une relation entre un responsable du traitement et un sous-traitant.

4.1. Généralités

4.1.1. Lorsqu'une partie agit en tant que responsable du traitement des données et l'autre partie en tant que sous-traitant, la première détient seule le pouvoir exclusif de déterminer les finalités et les moyens du traitement des données à caractère personnel reçues de l'autre partie ou par son intermédiaire et sera responsable du respect et de l'exécution de ses obligations en vertu de la législation sur la protection des données, à savoir :

a) garantir que les données à caractère personnel partagées fournies ou mises à disposition dans le cadre du contrat sont exactes et actuelles ;
b) fournir uniquement des instructions relatives au traitement des données à caractère personnel qui soient licites ;

c) garantir qu'elle dispose d'une base juridique appropriée pour le traitement des données à caractère personnel partagées telle que décrite dans le présent APD et/ou dans le contrat ;
d) veiller à ce que toutes notifications nécessaires relatives au traitement équitable (communément dénommées « avis de confidentialité » ou « politiques de confidentialité ») soient fournies aux personnes concernées par le traitement des données lors de la collecte de leurs données à caractère personnel afin

de permettre le traitement licite (y compris collecte et partage) des données à caractère personnel partagées aux fins énoncées dans le contrat et/ou l'APD ;

e) garantir que – sauf si une autre base juridique prévue par les lois sur la protection des données justifie la licéité du traitement – tout consentement nécessaire de la personne concernée au traitement sera obtenu et enregistré et, au cas où une personne concernée révoquerait son consentement, veiller à ce qu'il en soit fait communication à l'autre partie

f) et mettre en œuvre et maintenir des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité approprié au risque (prenant en compte la nature, la portée, le contexte et les finalités du traitement), notamment au risque de traitement non autorisé ou illicite, de perte accidentelle, de destruction ou de détérioration de ces données à caractère personnel.

4.1.2. Le responsable du traitement s'engage à ne pas fournir au sous-traitant des données à caractère personnel d'une catégorie spécifique (telles que des données relatives à la santé) non nécessaires à l'exécution des prestations de service.

5. Obligations applicables à une partie agissant en tant que sous-traitant

Le présent paragraphe 5 s'applique dans le cas où une partie agit en tant que sous-traitant pour le compte de l'autre partie. À cette fin, lorsqu'une partie traitera des données à caractère personnel pour le compte de l'autre partie, elle devra se conformer à ses obligations en vertu de la législation sur la protection des données applicable dans les juridictions où elle exerce ses activités, ainsi qu'aux obligations visées au présent APD, ainsi qu'exposé ci-après.

5.1. Sécurité des données

5.1.1. Le sous-traitant

a) satisfera aux normes de sécurité des données communiquées par l'autre partie et/ou convenues avec elle ;

b) conservera toutes données à caractère personnel dans un environnement sécurisé afin de garantir qu'elles ne seront pas divulguées à des tiers (sauf dans les cas autorisés par le contrat) ou utilisées de manière abusive par des tiers ;

c) prendra toutes mesures appropriées, compte tenu de la nature et des risques présentés par le traitement des données, afin d'assurer qu'aucun incident lié à la sécurité des données ne puisse se produire

d) et ne contournera pas les technologies utilisées par nous ou par des tiers pour protéger les contenus accessibles par l'intermédiaire des prestations de service.

5.1.2. La partie agissant en tant que sous-traitant s'engage à mettre en œuvre toutes mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel, en tenant compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement des données, ainsi que des risques, du degré de probabilité et de gravité impactant les droits et libertés des personnes concernées afin de garantir un niveau de sécurité approprié au risque, ce qui implique notamment ce qui suit :

a) lorsque le commerçant agit en tant que sous-traitant, il est tenu de prendre toutes mesures techniques et organisationnelles appropriées, y compris, mais sans qu'elles y soient circonscrites, les mesures énoncées à l'Annexe 3, afin de garantir un niveau de sécurité approprié pour les données à caractère personnel (notamment pour les protéger de toute destruction, perte ou altération accidentelles ou illicites, ainsi que de toute divulgation ou tout accès non autorisés).

b) Lorsque Planet agit en tant que sous-traitant, Planet applique les mesures techniques et organisationnelles suivantes, disponibles à l'adresse https://www.weareplanet.com/technical-and-organisational-measures, dont un tableau récapitulatif figure à l'Annexe 2.

5.1.3. Sans restriction de l'essentialité de toute autre divulgation de données à caractère personnel, toute violation du présent paragraphe 5.1 sera considérée comme violation substantielle du contrat.

5.2. Confidentialité et secret

5.2.1. Le sous-traitant s'engage à satisfaire à son obligation de confidentialité concernant les données à caractère personnel auxquelles il a eu accès dans le cadre du présent contrat. À cette fin, le sous-traitant s'assurera que les personnes autorisées à traiter les données à caractère personnel se sont engagées à en respecter la confidentialité ou sont soumises à des obligations légales de confidentialité et que tous leurs employé(e)s respectifs ont été formés conformément à leurs responsabilités respectives en vertu de la législation sur la protection des données.

5.3. Instructions du responsable du traitement des données

5.3.1. Le sous-traitant traitera les données à caractère personnel uniquement sur instruction écrite du responsable du traitement (y compris les instructions documentées dans le présent APD) dans le cadre des services fournis en vertu du contrat et ne devra pas les utiliser à d'autres fins que celles spécifiées dans le présent APD et/ou le contrat. Le sous-traitant s'engage à informer le responsable du traitement par écrit dans les plus brefs délais s'il estime qu'une instruction du responsable du traitement est susceptible d'enfreindre la législation sur la protection des données.

5.4. Sous-traitance

5.4.1. Le sous-traitant est autorisé à faire appel à des sous-traitants ultérieurs pour l'exécution des activités prévues dans le présent contrat. Néanmoins, si, après la date du présent addendum, de nouveaux sous-traitants ultérieurs sont mandatés par le sous-traitant, le responsable du traitement des données pourra acceptablement s'opposer, pour des motifs légitimes, à tout changement ou tout recours à un nouveau sous-traitant ultérieur en en informant le sous-traitant par écrit dans les dix (10) jours suivant la notification d'un nouveau sous-traitant ultérieur. En l'absence d'objection, le sous-traitant ultérieur est réputé avoir été accepté.

5.4.2. En particulier, le commerçant reconnaît que les sous-traitants ultérieurs de Planet sont essentiels à la fourniture des services et que s'il s'oppose à ce que Planet ait recours à un sous-traitant ultérieur, Planet, nonobstant toutes dispositions contraires figurant au contrat (y compris le présent addendum), ne sera alors pas tenue de fournir au commerçant le service pour lequel elle a recours à ce sous-traitant ultérieur.

5.4.3. Les sous-traitants ultérieurs de Planet et du commerçant figurent à l'Annexe 4. En signant le présent addendum, Planet et le commerçant autorisent respectivement l'autre partie à faire appel à ces sous-traitants ultérieurs.

5.4.4. Le sous-traitant conclura avec ses sous-traitants ultérieurs un accord écrit leur imposant des obligations conformes aux obligations prévues dans le présent addendum et/ou dans le contrat. Si un sous-traitant ultérieur manque à ses obligations en matière de protection des données telles que visées au présent contrat, le sous-traitant assumera, vis-à-vis du responsable du traitement, la responsabilité des actes et omissions de son sous-traitant ultérieur dans la même mesure que s'il avait lui-même directement exécuté le service concerné aux termes du contrat.

5.4.5. Le sous-traitant conclura avec le sous-traitant ultérieur une clause de tiers bénéficiaire en vertu de laquelle, dans le cas où le sous-traitant aurait disparu, cessé d'exister en droit ou serait devenu insolvable, le responsable du traitement sera habilité à résilier le contrat du sous-traitant ultérieur et à lui donner instruction d'effacer ou de restituer toutes données à caractère personnel.

5.5. Assistance au responsable du traitement des données, compliance et audits

5.5.1. Par la mise en œuvre des mesures techniques et organisationnelles appropriées et dans toute la mesure du possible, le sous-traitant apportera son assistance au responsable du traitement dans le traitement des demandes de personnes concernées qu'il pourrait recevoir. Le responsable du traitement des données sera habilité, à tout moment, à donner par écrit instruction au sous-traitant de cesser de répondre à ces demandes de personnes concernées. Lorsque le sous-traitant recevra une demande d'une personne concernée, il y répondra conformément à la législation applicable en matière de protection des données. Le responsable du traitement des données n'est pas sans savoir que le traitement de ces demandes par le sous-traitant pour le compte du responsable du traitement des données n'implique aucune exemption des obligations légales

imposées par la législation applicable en matière de protection des données ni aucune renonciation à ces obligations.

5.5.2. Le sous-traitant, en tenant compte de la nature du traitement et des informations dont il dispose, assistera également le responsable du traitement dans la garantie du respect des obligations prévues par la législation sur la protection des données qui s'appliquent au traitement des données visé par le présent ATD, y compris les notifications à une autorité de contrôle ou aux personnes concernées, le processus de réalisation d'une analyse d'impact relative à la protection des données et la consultation préalable des autorités de contrôle.

5.5.3. Le sous-traitant mettra à la disposition du responsable du traitement toutes informations nécessaires pour apporter la preuve du respect de ses obligations respectives visées au présent addendum et autorisera les audits de données, y compris les inspections, et y contribuera, si le responsable du traitement le demande.

5.5.4. Une fois par an, avec un préavis d'au moins 30 jours, le responsable du traitement des données pourra effectuer, à ses frais, tout audit visant à confirmer le respect de la législation sur la protection des données. L'audit sera effectué soit par le personnel de l'une des parties, soit par une entité indépendante choisie par la partie chargée de l'audit et dont les membres indépendants posséderont les qualifications professionnelles requises, seront liés par une obligation de confidentialité et n'appartiendront pas à une société directement concurrente de l'une des parties en ce qui concerne les services. Les parties conviennent

a) que l'audit ne devra pas inclure de données financières ou personnelles ne se rapportant pas directement et exclusivement à chacune des parties, ni aucune information susceptible d'affecter les systèmes et données de sécurité de chacune des parties (c'est-à-dire de présenter un risque pour la confidentialité des informations), ni le code source des programmes informatiques utilisés dans le cadre de la prestation des services ;
b) que l'auditeur, sans autorisation préalable, ne devra pas copier tout ou partie d'un document, d'un fichier, de données ou d'informations, ni prendre de photos, ni scanner, ni enregistrer des fichiers audio/vidéo ou informatiques/des programmes
c) et que l'audit devra avoir lieu pendant les heures de travail et être réalisé de manière à ne pas perturber les activités ou les prestations de service de la partie auditée.

5.6. Transferts internationaux de données

5.6.1. Le sous-traitant ne pourra traiter les données à caractère personnel qu'au sein de l'EEE, au Royaume-Uni ou en Suisse (selon le cas) ou dans d'autres pays reconnus par la Commission Européenne, l'ICO ou le PFPDT suisse (selon le cas) comme garants d'un niveau adéquat de protection des données à caractère personnel en ce qui concerne la confidentialité des données et les droits et libertés fondamentaux des personnes.

5.6.2. Lorsque le sous-traitant transférera ou exportera des données à caractère personnel vers un pays tiers situé hors de l'EEE, du Royaume-Uni ou de la Suisse (selon le cas) dépourvu d'un niveau de protection adéquat tel que déclaré par la Commission Européenne, l'ICO ou le PFPDT suisse (selon le cas), le sous-traitant devra satisfaire à ses obligations en vertu de la législation sur la protection des données (i) en faisant usage de tous mécanismes appropriés de contrôle des transferts reconnus comme garantie adéquate par la législation sur la protection des données ou (ii) en soumettant les conditions de ce transfert aux clauses contractuelles types qui seront intégrées au présent APD.

5.6.3. En outre, le sous-traitant mettra en œuvre et intégrera au présent APD toutes mesures supplémentaires adéquates qui soient pertinentes en fonction du risque réglementaire du pays de destination, garantissant ainsi un niveau de protection des données équivalent, pour l'essentiel, au niveau de protection en vigueur dans l'EEE, au Royaume-Uni ou en Suisse, selon le cas.

5.6.4. Dans la mesure où le sous-traitant s'appuie sur un mécanisme légal spécifique pour normaliser les transferts internationaux de données et que ce mécanisme est ensuite modifié, révoqué ou invalidé par un Tribunal compétent, les parties conviennent de coopérer en toute bonne foi afin de trouver un autre mécanisme approprié pouvant légalement soutenir le transfert.

5.7. Incidents liés à la sécurité des données

5.7.1. Lorsque le sous-traitant aura connaissance d'un incident lié à la sécurité des données ayant une incidence significative sur le traitement des données à caractère personnel objet du contrat, il en informera sans délai le responsable du traitement, coopérera à tout moment avec celui-ci et suivra ses instructions concernant cet incident lié à la sécurité des données, afin de permettre au responsable du traitement de mener une enquête sur l'incident, de formuler une réponse appropriée et de prendre des mesures supplémentaires en ce qui concerne ledit incident.

5.7.2. En cas de survenance d'un incident lié à la sécurité des données, ou s'il y a lieu de soupçonner qu'un incident lié à la sécurité des données s'est produit ou pourrait se produire, le sous-traitant en informera par écrit le responsable du traitement dans les plus brefs délais, en lui fournissant toutes informations pertinentes concernant les détails de l'incident, afin de lui permettre de satisfaire à la législation sur la protection des données. Les informations pertinentes relatives à l'incident lié à la sécurité des données comprendront :

a) le nom, le nom commercial et les informations censées avoir été impactées ;
b) une description de la nature de l'incident, y compris, si possible, les catégories et le nombre approximatif de personnes concernées ;
c) le nom et les coordonnées du délégué à la protection des données du sous-traitant ou d'un autre point de contact où des informations complémentaires pourront être obtenues ;
d) le nom et les coordonnées du délégué à la protection des données du sous-traitant ou d'un autre point de contact où des informations complémentaires pourront être obtenues ;
e) une description de ses conséquences probables de l'incident ;
f) une description des mesures prises ou proposées par le sous-traitant pour y remédier, y compris, le cas échéant, des mesures visant à atténuer ses éventuelles incidences négatives
g) et une copie de toute la correspondance s'y rapportant, y compris toute correspondance avec toutes personnes concernées.

5.8. Enregistrement des traitements

5.8.1. Le sous-traitant conservera une trace écrite de toutes catégories d'activités de traitement des données effectuées pour le compte du responsable du traitement lorsqu'il agira en tant que sous-traitant, y compris

a) le nom et les coordonnées du responsable du traitement pour le compte duquel il agit, de tout sous-traitant ultérieur et, le cas échéant, du délégué à la protection des données ;
b) les catégories d'activités de traitement des données effectuées pour le compte du responsable du traitement ou de la personne concernée ;
c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés par la législation sur la protection des données ;
d) dans toute la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

5.9. Restitution ou destruction de données à caractère personnel

5.9.1. Après prestation du service convenu contractuellement ou à la résiliation du contrat, le sous-traitant, à la discrétion du responsable du traitement et selon les modalités et délais indiqués par ce dernier, devra restituer et/ou détruire toutes données à caractère personnel auxquelles il aura eu accès pendant la durée de la relation contractuelle, ainsi que tout autre document considéré comme confidentiel, sauf si une obligation ou un obstacle juridique en dispose autrement.

5.9.2. Nonobstant ce qui précède, si aucune instruction n'est reçue du responsable du traitement dans les trois mois suivant la prestation des services ou la résiliation du contrat, les données à caractère personnel seront détruites. Le responsable du traitement pourra demander au sous-traitant de fournir un certificat écrit attestant de la destruction des données à caractère personnel et des documents détruits.

5.9.3. Sous réserve de l'acceptation d'un devis par le responsable du traitement, le sous-traitant fournira les données à caractère personnel au responsable du traitement ou à tout tiers désigné par celui-ci, dans un format habituel sur le marché, afin de poursuivre le traitement des données à caractère personnel.

6. Divers

6.1. Le présent addendum constitue l'intégralité de l'accord conclu entre Planet et le commerçant en ce qui concerne son objet et remplace tout accord antérieur que les parties auraient pu conclure à ce sujet.

6.2. Sauf modification ou complément spécifique apporté(e) par les termes du présent addendum, le contrat et toutes les dispositions qu'il contient ou les termes de tout autre contrat ou document qui y est mentionné restent pleinement en vigueur et valides.

6.3. En cas de conflit entre les dispositions du présent addendum et celles de toute autre modification ou tout autre addendum et/ou de l'accord relatif au traitement des données à caractère personnel, les dispositions du présent addendum prévaudront.

6.4. La loi applicable et le domicile de compétence en ce qui concerne le présent addendum sont régis par le droit en vigueur et le domicile de compétence prévu au contrat.

EN FOI DE QUOI, les parties aux présentes ont fait signer et remettre le présent addendum par leurs représentants dûment autorisés à la date indiquée ci-dessus.

Planet	Commerçant
En la personne de : _____	En la personne de : _____
Nom :	Nom :
Titre :	Titre :

APPENDIX 1

Finalités du traitement

Les parties conviennent que Planet pourra utiliser les données à caractère personnel (ou, le cas échéant, les données à caractère personnel partagées) au nom de la personne concernée aux fins suivantes :

a) satisfaire à ses obligations en vertu du contrat (par exemple, permettre la gestion des transactions) ;
b) satisfaire à ses obligations aux termes de la législation applicable et aux exigences et demandes des autorités de contrôle (par exemple, vérifier l'identité des personnes concernées) ;
c) pour ses intérêts légitimes (par exemple, améliorer notre feed-back sur les services fournis).

Les parties s'engagent à ce que les données à caractère personnel (ou, le cas échéant, les données à caractère personnel partagées) ne soient jamais vendues ni fournies à des tiers sans l'autorisation écrite préalable des personnes concernées.

Rôles en matière de protection des données

Service	Planet	Commerçant	Catégorie de données et données à caractère personnel généralement traitées
Portail	Sous-traitant	Responsable	Données relatives aux clients du commerçant qui utilisent les services, notamment numéro PAN [Numéro de compte principal], code CVV [Code de sécurité unique], date d'expiration et code postal, lorsque ces données sont nécessaires à des fins de vérification. Pour l'APM [Méthode alternative de paiement], seul le numéro de compte est traité.
Proxy PCI [Payment Card Industry]	Sous-traitant	Responsable	Données relatives aux clients du commerçant qui utilisent les services, notamment numéro PAN, date d'expiration de la carte, code CVV.
Acquisition	Contrôleur	Responsable	Données relatives aux clients du commerçant qui utilisent les services, notamment numéro PAN, code CVV, date d'expiration et code postal, lorsque ces données sont nécessaires à des fins de vérification. Pour l'APM, seul le numéro de compte est traité.
Location d'équipement	Sous-traitant	Responsable	Certaines données limitées relatives aux clients du commerçant qui utilisent les services liés aux opérations de paiement effectuées à l'aide de l'équipement, notamment le montant des transactions et le code d'autorisation.
Achat d'équipement	Sous-traitant	Responsable	Certaines données limitées relatives aux clients du commerçant qui utilisent les services liés aux opérations de paiement effectuées à l'aide de l'équipement, notamment le montant des transactions et le code d'autorisation (le cas échéant).
Conversion des devises	Sous-traitant	Responsable	Données relatives aux clients du commerçant qui utilisent les services, notamment adresse IP (uniquement pour la DCC [Conversion dynamique]), numéro d'identification de la carte (6 premiers chiffres), données de carte tokenisées, informations sur l'appareil.
Remboursement de TVA	Contrôleur	Sous-traitant	Données relatives aux clients du commerçant qui utilisent les services, notamment le numéro PAN, le code CVV, la date d'expiration et le code postal, lorsque ces données sont nécessaires à des fins de vérification. Pour l'APM, seul le numéro de compte est traité.
Logiciel de gestion des cartes-cadeaux	Sous-traitant	Responsable	Données relatives aux clients du commerçant qui utilisent les services : nom, adresse E-mail et adresse postale (si une carte-cadeau physique est émise).

Logiciel de vente au détail	Sous-traitant	Responsable	Données relatives aux clients du commerçant qui utilisent les services, notamment nom, adresse E-mail, numéro de téléphone, adresse postale ; informations de connexion de l'utilisateur (adresse IP, type de navigateur) ; informations de facturation de l'utilisateur (coordonnées, quatre derniers chiffres de la carte de crédit et type de mode de paiement).
Tous les services, le cas échéant	Sous-traitant	Responsable	Données relatives au personnel du commerçant, notamment : noms, adresses e-mail professionnelles, numéros de téléphone, fonctions, à télécharger sur la plateforme de formation afin d'organiser et de gérer les services de formation demandés par le commerçant.

ANNEXE 2

Lorsque Planet traite des données à caractère personnel (ou, le cas échéant, des données à caractère personnel partagées), elle applique les mesures techniques et organisationnelles suivantes, disponibles à l'adresse https://www.weareplanet.com/technical-and-organisational-measures, dont un tableau récapitulatif est présenté ci-dessous :

Catégorie	Sous-catégorie	Mesure
Programmes et politiques de sécurité	Programme de sécurité	Planet maintient et applique un programme de sécurité qui régit la manière dont Planet gère la sécurité.
	Programme de confidentialité	Planet maintient et applique un programme de confidentialité qui régit la collecte, l'utilisation et le partage des données à caractère personnel.
Gestion des risques et des actifs	Évaluations du risque	Planet gère les risques de manière proactive grâce à son cadre de gestion des risques entrepreneuriaux et à son solide modèle à trois lignes.
	Gestion des actifs	Planet maintient et applique un programme de gestion des actifs qui classe et contrôle de manière appropriée les actifs matériels et logiciels tout au long de leur cycle de vie.
Formation et contrôles du personnel	Reconnaissance de responsabilité	Tous les employés de Planet, ainsi que les prestataires indépendants susceptibles d'avoir accès à des données, y compris ceux qui traitent des données à caractère personnel, reconnaissent leurs responsabilités en matière de sécurité et de confidentialité des données conformément aux politiques de Planet.
Formation et sensibilisation	Formations annuelles sur la sécurité et la confidentialité	Les employés de Planet suivent chaque année une formation de sensibilisation au RGPD, au KYC [Know your customer], à la lutte contre le blanchiment d'argent et à la sécurité de l'information.
Gestion du réseau et des opérations	Politiques et procédures	Planet met en œuvre des politiques et des procédures pour la gestion du réseau et des opérations. Ces politiques et procédures concernent le renforcement de la sécurité, le contrôle des évolutions, la séparation des tâches, la séparation des environnements de développement et de production, la gestion de l'architecture technique, la sécurité du réseau, la protection contre les logiciels malveillants, la protection des données en transfert et au repos, l'intégrité des données, le cryptage, les protocoles d'audit et la séparation des réseaux.
	Évaluations de la vulnérabilité	Planet effectue régulièrement des évaluations de vulnérabilité et des tests de pénétration sur ses systèmes et ses applications, y compris ceux qui traitent des données à caractère personnel.

Catégorie	Sous-catégorie	Mesure
Contrôles techniques d'accès	Contrôle d'accès	Planet met en œuvre des mesures visant à empêcher l'utilisation des systèmes de traitement des données par des personnes non autorisées.
	Contrôle de l'accès aux données	Planet met en œuvre des mesures visant à garantir que les personnes autorisées à utiliser un système de traitement des données n'auront accès qu'aux données à caractère personnel autorisées dans le cadre de leurs droits d'accès et que les données à caractère personnel ne pourront être lues, copiées, modifiées ou supprimées sans autorisation.
Contrôles physiques d'accès	Sécurité des centres de données	Planet fait appel à des prestataires de services tiers de confiance pour héberger son infrastructure de production. Planet dépend de ces tiers pour superviser les contrôles d'accès physique aux installations des centres de données gérés par leurs soins.
	Sécurité des bureaux	L'accès physique aux bureaux de Planet est contrôlé à l'aide de mécanismes tels que l'enregistrement des visiteurs, des serrures électroniques, des systèmes d'alarme et des salles de stockage sécurisées.
	Audits réalisés par des tiers	Planet examine les rapports d'audit réalisés par des tiers afin de vérifier que ses prestataires de services maintiennent des contrôles d'accès physiques appropriés pour nos centres de données gérés.
Contrôles de disponibilité	Disponibilité	Planet a mis en place des mesures visant à garantir le rétablissement rapide de la disponibilité et de l'accès aux données à caractère personnel en cas d'incident physique ou technique.
Contrôles de divulgation	Divulgation	Planet met en œuvre des mesures visant à garantir que les données à caractère personnel ne pourront être lues, copiées, modifiées ou supprimées sans autorisation lors de leur transmission électronique, de leur transport ou de leur stockage sur des supports (manuels ou électroniques).
Contrôles de séparation	Séparation	Planet met en œuvre des mesures visant à garantir que les données à caractère personnel collectées à des fins différentes pourront être traitées séparément.
Certifications	Compliance PCI	Planet s'engage à fournir ses services dans le respect des normes de compliance PCI-DSS [Payment Card Industry Data Security Standard], telles qu'elles s'appliquent à nos offres.
Cryptage	Mécanismes de cryptage	Au cours de différentes phases, Planet a recours à des mécanismes de cryptage des données afin de réduire le risque d'accès non autorisé aux données au repos et en transfert. De plus, l'accès aux clés cryptographiques de Planet est limité à un groupe restreint de membres du personnel Planet autorisés.
Gestion et notification des incidents liés à la sécurité des données	Gestion des incidents	Planet met en œuvre un programme de gestion des incidents liés à la sécurité des données qui régit la manière dont Planet gère les incidents.
Sauvegarde et suppression des données	Conservation des données	Planet met en œuvre et maintient des politiques et procédures de sauvegarde des données relatives aux données à caractère

Catégorie	Sous-catégorie	Mesure
		personnel et révise ces politiques et procédures en fonction des besoins.

ANNEXE 3

Lorsque Planet agit en tant que responsable du traitement des données et le commerçant en tant que sous-traitant, le commerçant est tenu de mettre en œuvre des mesures techniques et organisationnelles afin de garantir un niveau de sécurité approprié au risque, dont font entre autres partie les mesures suivantes :

1. Définir les fonctions et les responsabilités du personnel chargé du traitement des données à caractère personnel et informer ce personnel de ses fonctions et responsabilités en matière de respect des lois et réglementations relatives à la protection des données ;
2. Définir les rôles et les profils des utilisateurs des applications et des systèmes par l'intermédiaire desquels les données à caractère personnel sont traitées, conformément aux fonctions et responsabilités établies, afin d'empêcher tout accès non autorisé aux données à caractère personnel ou aux ressources. Ce système de contrôle d'accès doit être garant de mécanismes appropriés d'identification et d'authentification des utilisateurs, tels que des mots de passe devant être périodiquement réinitialisés, des données biométriques, une authentification multifactorielle, le blocage automatique de l'utilisateur après un nombre prédéfini de tentatives de connexion infructueuses ;
3. Appliquer des mesures permettant la pseudonymisation et le cryptage des données à caractère personnel ;
4. Mettre en place des registres de contrôle et d'accès aux fichiers et aux supports contenant des données à caractère personnel, qui devront également comporter des mécanismes visant à en restreindre l'accès ;
5. Appliquer des mesures automatisées qui restreignent cet accès aux utilisateurs non autorisés ou lorsque la période de pertinente de sauvegarde a expiré, par exemple au moyen de techniques d'effacement et de pseudonymisation des données ;
6. Mettre en œuvre des procédures visant à limiter l'accès physique aux installations hébergeant les systèmes d'information ou les supports physiques ;
7. Appliquer des mesures visant à garantir la confidentialité, l'intégrité, la disponibilité et la résilience continues des systèmes et des services ;
8. Mettre en œuvre des procédures de récupération des données à caractère personnel en cas de destruction, de perte ou d'altération, sous la supervision et sous réserve de l'approbation du délégué à la protection des données ;
9. Mettre en œuvre des procédures pour détecter, évaluer et, si nécessaire, signaler tout incident lié à la sécurité des données susceptible d'affecter les droits et les libertés des personnes concernées ;
10. Réaliser des examens de conformité périodiques, définir et mettre en œuvre des plans d'action visant à atténuer les risques détectés ;
11. Appliquer toutes autres mesures techniques et organisationnelles adéquates afin de garantir un niveau de sécurité approprié au risque.

ANNEXE 4

La liste des sous-traitants ultérieurs de Planet peut être consultée à l'adresse suivante : https://www.weareplanet.com/legal/subprocessor-and-service-provider-list.

Les sous-traitants ultérieurs du commerçant sont les suivants :