Mise à jour de l'addenda sur la protection des données

Date d'entrée en vigueur pour les marchands actuels ou dès maintenant pour les marchands qui ouvrent leur compte après le 1er novembre 2023 (« date d'entrée en vigueur »).

Le présent Addenda sur la protection des données (« Addenda ») est conclu entre le Marchand et PayPal (collectivement les « Parties »). Le présent Addenda fait partie du Contrat entre le Marchand et PayPal (le « Contrat ») conformément à la section « Effet du présent Addenda » ci-dessous.
Les termes en majuscules utilisés mais non définis dans le présent addenda ont le sens qui leur est conféré dans le Contrat.

I. EFFET DU PRÉSENT ADDENDA

Le présent addenda constitue une modification et une partie intégrante du Contrat. Il prend effet à la date d'entrée en vigueur du Contrat.

II. GÉNÉRALITÉS

1\. Définitions
Les termes ci-après ont les significations suivantes lorsqu'ils sont utilisés dans le présent Addenda :

- a. « Contrat » désigne le Contrat de services ou le Contrat Marchand (selon le cas) conclu entre PayPal et le Marchand. b. Un « Contrôleur » (également appelé « responsable du traitement des données ») désigne une entité qui détermine les objectifs et les moyens du Traitement des données à caractère personnel. Si ce terme (ou un terme similaire ayant les mêmes fonctions) est déjà défini par les Lois sur la protection des données en vigueur, le terme « Contrôleur », tel que mentionné dans les présentes, aura la signification prévue par la Loi sur la protection des données en vigueur, y compris la signification d'une « Entreprise », le cas échéant, telle que définie dans la Loi californienne de 2018 sur la protection de la vie privée des consommateurs.
  c. « Données du Marchand » désignent toutes les Données personnelles que PayPal reçoit du Marchand ou du Bénéficiaire relatives au Marchand, à un Bénéficiaire, ou liées à l'utilisation des

Services Hyperwallet par le Marchand, existant avant ou après la date du présent Contrat.

d. « Lois sur la protection des données » désignent toutes les lois, les réglementations, les directives, les exigences réglementaires et codes de pratique en matière de protection des données applicables à la fourniture des Services PayPal en vertu du présent Contrat, y compris toute modification de ceux-ci et toute réglementation ou tout instrument associé (exemple : qui peut inclure, sans s'y limiter, le Règlement général sur la protection des données (UE) 2016/679 (« RGPD »), le Règlement général sur la protection des données du Royaume-Uni (« RGPD du Royaume-Uni »), la Loi britannique de 2018 sur la protection des données, la loi californienne de 2018 sur la protection de la vie privée des consommateurs, Cal. Civ. Code § 1798.100 et suivants (« CCPA »), et ses dispositions d'application, la Loi australienne de 1988 sur la protection de la vie privée (Cth), la loi sur la protection des renseignements personnels et les documents électroniques (Canada), l'Ordonnance sur les renseignements personnel (la vie privée) (Cap.486) (Hong Kong), la Loi générale brésilienne sur la protection des données, la Loi Fédérale N° 13 709/2018, et la Loi de 2012 sur la protection des données personnelles (Singapour)).

e. « PayPal Group » désigne PayPal, Inc. et toutes les sociétés que PayPal, ou son/ses successeur(s), possède ou contrôle directement ou indirectement. « Bénéficiaire » désigne une personne ou une entreprise recevant un paiement par le biais des Services Hyperwallet utilisés par le Marchand.

g. « Une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment au moyen d'un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou au moyen d'un ou plusieurs éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique.

h. Les termes « Traitement » ou « traité » ou « en cours de traitement » désignent : toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, y compris la collecte, l'enregistrement, la conservation, le partage, l'organisation, le stockage, l'accès, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, la divulgation, la diffusion, la mise à disposition, l'alignement, la combinaison, le blocage, la suppression, la suppression ou la destruction.

2. PayPal en tant que contrôleur
PayPal doit se conformer aux exigences des Lois sur la protection des données applicables aux contrôleurs en ce qui concerne l'utilisation des Données du Marchand (notamment, sans s'y limiter, en mettant en œuvre et en appliquant en permanence toutes les mesures de sécurité appropriées relatives au Traitement des données du Marchand) et ne doit rien faire, ni autoriser sciemment une action susceptible d'exposer le marchand à une violation des Lois sur la protection des données. PayPal ne transfère les Données du Marchand qu'à des tiers, des sous-traitants ou des membres du Groupe PayPal qui signent des accords écrits stipulant les conditions de protection des Données du Marchand au moins aussi explicites que les conditions énoncées dans le présent Addenda. Dans le cas où le Marchand choisit une solution de paiement où un bénéficiaire n'est pas tenu d'ouvrir un compte via la solution hébergée par Hyperwallet, le Marchand accepte de présenter la politique de confidentialité d'Hyperwallet (https://pay.hyperwallet.com/hw2web/consumer/page/privacyAgreement.xhtml) à ses bénéficiaires avant de partager les données personnelles de ses bénéficiaires avec PayPal.

3. Traitement des données du Marchand dans le cadre des Services Hyperwallet
Les Parties reconnaissent et acceptent que lorsque PayPal fournit des Services Hyperwallet au Marchand, ce dernier et PayPal sont tous deux des Contrôleurs indépendants pour toutes les Données du Marchand traitées dans le cadre des Services Hyperwallet. À ce titre, PayPal détermine indépendamment l'objectif et les moyens du traitement de ces Données marchandes et ne constitue pas un contrôleur conjoint avec le Marchand en ce qui concerne les données du Marchand. Les Parties reconnaissent et acceptent que PayPal peut utiliser, reproduire et traiter les Données du Marchand et les données relatives aux transactions de paiement pour les raisons précises suivantes :

- a. Selon que cela est raisonnablement nécessaire, pour fournir et améliorer les Services Hyperwallet destinés au Marchand et à ses Bénéficiaires, y compris les outils de protection contre la fraude ;
  b. Pour surveiller, prévenir et détecter les transactions de paiement frauduleuses, et pour éviter tout préjudice au Marchand, à PayPal et à des tiers ;
  c. Pour se conformer aux obligations légales ou réglementaires applicables au Traitement et à la conservation des données de paiement auxquelles PayPal est soumis, y compris les obligations

applicables en matière de lutte contre le blanchiment d'argent et de vérification d'identité ;
d. Pour analyser, développer et améliorer les produits et services de PayPal ;
e. Pour une utilisation interne, y compris, entre autres, pour l'analyse des données et les mesures;
f. Pour compiler et divulguer les Données du Marchand et les données sur les transactions de paiement dans leur ensemble lorsque les Données personnelles ou les données d'utilisateur du Marchand ne sont pas identifiables, y compris le calcul des moyennes du Marchand par région ou par secteur ;
g. Pour se conformer aux exigences légales applicables et aider les organismes chargés de l'application de la loi en répondant aux demandes de divulgation d'informations conformément aux lois ; et
h. Pour toute autre raison pour laquelle PayPal notifie le Marchand, à condition que cette raison soit conforme aux Lois sur la protection des données en vigueur.

4. Assistance mutuelle

Les parties conviennent de coopérer l'une avec l'autre selon les besoins pour permettre à l'autre partie de s'acquitter convenablement de sa responsabilité en tant que Contrôleur indépendant en vertu des Lois sur la protection des données. Les parties conviennent que, dans la mesure où le Marchand reçoit une demande d'accès d'un bénéficiaire ou si un bénéficiaire se prévaut de ses droits en vertu des lois sur la protection des données, le Marchand doit répondre directement à la demande d'accès de ce bénéficiaire. Le Marchand doit également informer les Bénéficiaires qu'ils peuvent exercer leurs droits en matière de données liées aux Services Hyperwallet auprès de PayPal conformément aux instructions de la Déclaration de confidentialité disponible à l'adresse https://www.hyperwallet.com/privacy-policy/ (qui peut être modifiée de temps à autre). En outre, si dans le cadre d'un incident de sécurité, PayPal détermine à sa discrétion qu'il doit notifier les bénéficiaires concernés, et qu'il ne dispose pas de toutes coordonnées de ces bénéficiaires pour effectuer cette communication, le Marchand doit alors s'efforcer de fournir à PayPal les informations dont il dispose sur ce Bénéficiaire dans le seul but de permettre à PayPal de se conformer aux obligations de notification applicables aux bénéficiaires concernés en vertu de la Loi sur la protection des données.

5. Partage transfrontalier des données

Les parties conviennent que PayPal peut transférer les données du marchand traitées en vertu du présent Contrat en dehors du pays où elles ont été collectées si nécessaire pour fournir les Services Hyperwallet. Si PayPal transfère des données du marchand protégées par la présente Annexe vers une juridiction pour laquelle l'autorité de réglementation compétente du pays dans lequel les données ont été collectées n'a pas émis de décision de conformité (une « Décision de conformité »), PayPal s'assurera que des mesures de protection appropriées ont été mises en œuvre pour le transfert des Données du Marchand conformément aux Lois sur la protection des données en vigueur. Pour se conformer au RGPD, PayPal s'appuie par exemple sur des règles d'entreprise contraignantes approuvées par les autorités de contrôle compétentes et sur d'autres mécanismes de transfert de données pour les transferts de données des Marchands à d'autres membres du groupe PayPal.

-
    - a. En ce qui concerne les transferts de données à un membre du Groupe PayPal résidant dans un pays qui ne bénéficie pas d'une Décision de conformité des bénéficiaires se trouvant dans l'Union européenne, en Suisse, dans l'Espace économique européen, et/ou dans leurs États membres et au Royaume-Uni, les Parties conviennent (i) dans la mesure du possible, que votre signature du Contrat sera considérée comme une signature et une acceptation de la Décision d'exécution (UE) 2021/914 de la Commission européenne du 4 juin 2021 relative aux Clauses contractuelles standard pour le transfert de données à caractère personnel vers des pays tiers conformément au RGPD (« Clauses de transfert de l'UE ») par le Marchand, en tant qu'exportateur de données et dans le rôle de contrôleur et qu'elle sera considérée comme une signature et une acceptation de l'Addenda britannique relatif aux Clauses de transfert de l'UE approuvé par le Commissaire à l'information du Royaume-Uni et adopté en vertu de l'article 119A de la Loi de 2018 sur la protection des données, en vigueur au Royaume-Uni (les « Clauses de transfert du Royaume-Uni »), en tant qu'exportateur de données (ii) dans la mesure où cela s'applique, la signature du Contrat par le membre du

Groupe PayPal sera considérée comme une signature et une acceptation des Clauses de transfert de l'UE par ce membre du Groupe PayPal, en tant qu'importateur de données et en tant que contrôleur, et sera considérée comme une signature et une acceptation des Clauses de transfert du Royaume-Uni, comme importateur de données ; et (iii) les parties seront soumises aux dispositions du Module 1 des Clauses de transfert de l'UE. Si la Commission européenne ou le Secrétaire d'État britannique (ou tout autre organisme britannique autorisé) révise et publie ensuite de nouvelles Clauses de transfert de l'UE ou Clauses de transfert du Royaume-Uni, selon le cas (ou si la Commission européenne ou le Secrétaire d'État britannique (ou tout autre organisme britannique autorisé) l'exige ou l'applique), les parties conviennent que ces nouvelles clauses de transfert de l'UE ou clauses de transfert du Royaume-Uni, selon le cas, remplaceront les présentes clauses de transfert de l'UE ou clauses de transfert du Royaume-Uni, selon le cas, et elles acceptent de prendre toutes les mesures nécessaires à la mise en œuvre de ces nouvelles clauses de transfert, selon le cas. Les Clauses de transfert de l'UE (module 1) et les Clauses de transfert du Royaume-Uni seront toutes deux incorporées dans l'accord par renvoi et considérées comme dûment exécutées entre les parties lors de l'entrée en vigueur du présent Contrat, sous réserve des précisions suivantes :

A) Clauses de transfert de l'UE

1. L’option 1 de la clause 17 (loi applicable) s’applique et les lois luxembourgeoises régissent les clauses de l'UE ;
2. Conformément à la clause 18 (Choix du forum et de la juridiction), les tribunaux luxembourgeois résoudront tout litige découlant des clauses de l’UE ; et
3. Les parties conviennent que les détails requis en vertu de l'Annexe sur les clauses de transfert de l'UE sont indiqués dans la pièce jointe 1.

B) Clauses de transfert du Royaume-Uni

1. Le Tableau 1 de la partie 1 (les Parties) doit être complétée par les informations contenues dans la pièce jointe 1, annexe 1.A (liste des Parties).
2. Le Tableau 2 de la Partie 1, (SCC, Modules et Clauses sélectionnés) doit être remplie en sélectionnant la deuxième option « les SCC approuvées de l'UE, y compris l'Annexe Information et avec uniquement les modules, clauses ou dispositions optionnelles suivants des SCC approuvées de l'UE rendus effectifs pour les besoins de cet Addenda » et en indiquant dans la ligne du Module 1 que la Clause 7 (Clause de jonction) et la Clause 11 (Option) ne s'appliquent pas.
3. Le Tableau 3 de la partie 1 (Informations de l'Annexe) doit être complété par les informations figurant à l'appendice 1, aux annexes 1.A, 1.B et II.
4. Partie 1, Tableau 4 (Fin du présent addenda en cas de modification de l'addenda approuvé), l'option « Importateur » doit être sélectionnée.
5. Partie 2 : Les clauses obligatoires de l'addenda approuvé, à savoir le modèle d'addenda B.1.0 publié par l'ICO et présenté au Parlement conformément à l'article 119A de la loi sur la protection des données de 2018 le 2 février 2022, tel qu'il est révisé en vertu de l'article 18 de ces clauses obligatoires, sont incorporées par renvoi dans le présent Contrat.

Pièce jointe 1
Annexe aux clauses de transfert de l'UE

A) Les éléments suivants sont applicables, dans la mesure requise, en vertu des Clauses de transfert de l'UE et des Clauses de transfert du Royaume-Uni

Annexe 1.A. Liste des Parties

Exportateur de données

- Nom et adresse : Nom et adresse : l'exportateur de données est le Marchand et l'adresse est celle indiquée dans le Contrat
- Nom, fonction et coordonnées de la personne-ressource : tels que prévus dans le Contrat
- Activités relatives aux données transférées en vertu de la Clause contractuelle standard: comme prévu dans le Contrat
- Signature et date : veuillez consulter la section « Transferts transfrontaliers » du présent Addenda.

- Rôle (Contrôleur/processeur) : contrôleur

Importateur de données

- Nom et adresse : L’importateur de données est le membre du groupe PayPal qui fournit les services conformément au Contrat et son adresse est celle indiquée dans le Contrat.
- Nom, fonction et coordonnées de la personne-ressource : tels que prévus dans le Contrat
- Activités pertinentes pour les données transférées en vertu de la clause contractuelle standard : comme prévu dans le Contrat. Signature et date : veuillez consulter la section « Transferts transfrontaliers » du présent Addenda.
- Rôle (Contrôleur/processeur) : contrôleur

Annexe 1.B. Description du transfert

Personnes concernées dont les Données personnelles sont transférées
Les données personnelles transférées se rapportent aux catégories de personnes concernées suivantes :

- Les clients, les employés et les autres contacts professionnels de l’exportateur de données.

Catégories de données personnelles transférées
Les données personnelles transférées peuvent contenir les catégories de données suivantes :

- Le nom du Marchand et du bénéficiaire, le montant de la transaction, la date et l'heure, les coordonnées du compte bancaire, les détails de la carte de paiement, le cryptogramme visuel, le code postal, le code du pays, l'adresse, l'adresse de courriel, le télécopieur, le numéro de téléphone, le site Web, les données d'expiration, les données d'expédition, le statut fiscal, l'identifiant unique du client, l'adresse IP, la localisation, les informations sur les représentants du client, les informations sur la propriété bénéficiaire, les détails commerciaux et d'autres informations requises pour la connaissance du client et toutes les autres données reçues par PayPal en vertu du Contrat.

Transfert de données sensibles (le cas échéant) et restrictions ou mesures de protection appliquées

Les données personnelles transférées concernent les catégories de données sensibles suivantes :

- Sans objet, sauf si le marchand configure le service pour collecter ces données.

Applique des restrictions et des mesures de protection :

- Sans objet, sauf si le marchand configure le service pour collecter ces données.

Nature du traitement
Tel qu'énoncé dans le Contrat.

Objectif(s) du/des transfert(s)
Le transfert est effectué aux fins suivantes :

- Exécuter les services fournis par l'importateur de données à l'exportateur de données conformément au Contrat.
- Identifier les activités frauduleuses et les risques affectant ou susceptibles d'affecter l'importateur de données, l'exportateur de données ou d'autres clients de l'importateur de données.
- Respecter les lois applicables à l’importateur de données.
- Tel qu’indiqué dans l’Addenda sur la protection des données

Durée de conservation des données à caractère personnel ou, si cela n'est pas possible, critères utilisés pour déterminer cette durée.
L'importateur de données ne conserve les données à caractère personnel qu'aussi longtemps que nécessaire compte tenu du but ou des buts pour lesquels elles ont été collectées (voir les buts ci-dessus). Pour déterminer la durée de conservation appropriée des données à caractère personnel, l'importateur de données tient compte de la quantité, de la nature et de la sensibilité des données à caractère personnel, du risque potentiel de dommage résultant d'une utilisation ou d'une divulgation non autorisée de celles-ci, des fins pour lesquelles les données à caractère personnel sont traitées et de la possibilité d'atteindre ces objectifs par d'autres moyens, ainsi que des exigences légales, réglementaires, fiscales, comptables ou autres qui s'appliquent.

Pour les transferts vers des (sous-)processeurs, précisez également l’objet, la nature et la durée du traitement
L'importateur de données peut partager des données à caractère

personnel avec des prestataires de services tiers qui fournissent des services et exercent des fonctions selon les instructions de l'importateur de données et en son nom. Ces fournisseurs de services tiers peuvent, par exemple, fournir un élément des Services proposés dans le cadre du Contrat, comme le Service vérification client, le traitement des transactions ou le Service clientèle, ou fournir un service à l'importateur de renseignements qui prend en charge les Services fournis dans le cadre du Contrat, comme le stockage. Lorsqu'il détermine la durée du traitement effectué par les fournisseurs de services tiers, l'importateur de données applique les critères indiqués ci-dessus dans la présente Annexe I.B.

Annexe 1.C. Autorité de surveillance
Conformément à la Clause 13(a) des Clauses de transfert de l'UE, l'autorité de surveillance responsable de la conformité de l'exportateur de données avec le règlement (UE) 2016/679 en ce qui concerne le transfert de données, comme indiqué, agira en tant qu'autorité de surveillance compétente.

Annexe II Mesures techniques et organisationnelles Il s'agit de mesures techniques et organisationnelles visant à assurer la sécurité des données

1. Pseudonymisation, cryptage et protection des données lors de leur transmission.
   Les politiques de PayPal garantissent le respect de ce principe et exigent l'utilisation de contrôles techniques pour prévenir le risque de divulgation des données personnelles. PayPal utilise le cryptage en transit et au repos pour toutes les données personnelles. Nous utilisons également des techniques de pseudonymisation standard de l'industrie, telles que la création de jetons, pour protéger les données personnelles, le cas échéant. PayPal dispose de politiques complètes qui prévoient des obligations et des processus clés pour protéger les données lorsqu'elles sont transférées au sein de l'entreprise et à l'extérieur avec des tiers.
2. Gestion du changement et continuité des activités
   Le processus de gestion des changements de PayPal protège la disponibilité et la résilience des données et des systèmes pendant tout leur cycle de vie en s'assurant que les changements sont planifiés, approuvés, exécutés et revus de manière appropriée. Le processus de gestion de la continuité des activités de l'entreprise fournit un cadre permettant de renforcer la résilience de

l'organisation et d'apporter une réponse efficace qui préserve les intérêts de ses principales parties prenantes.

3. Reprise après sinistre.
   Le programme résilient de reprise après sinistre de PayPal prévoit des processus de récupération des informations ou des systèmes technologiques en cas de perturbation importante, en mettant l'accent sur les systèmes informatiques qui soutiennent les processus commerciaux essentiels et les activités des clients. Les infrastructures technologiques de PayPal sont hébergées dans plusieurs centres de données sécurisés, avec des fonctionnalités principales et secondaires, chacun étant équipé d'une infrastructure de réseau et de sécurité, de serveurs d'applications et de bases de données dédiés et d'un espace de stockage.
4. Test, inspection et évaluation réguliers de l'efficacité des mesures techniques et organisationnelles
   PayPal planifie, exécute et communique régulièrement les résultats du programme de test de la société afin d'évaluer l'efficacité de ses mesures technologiques et organisationnelles. Le programme est géré par notre équipe chargée des risques d'entreprise et de la conformité, qui collabore avec les parties prenantes concernées pour obtenir et évaluer les informations requises pour les tests, les rapports et les mesures correctives nécessaires.
5. Identification et autorisation de l'utilisateur.
   Les processus de gestion des accès de PayPal exigent que les utilisateurs se connectent au réseau de l'entreprise à l'aide d'un Identifiant de compte du réseau d'entreprise unique et d'un mot de passe pour l'identification et l'authentification de l'utilisateur avant d'accéder à toute autre application concernée. Des politiques automatisées concernant la composition, la longueur, la modification, la réutilisation et le verrouillage des mots de passe sont appliquées. L'accès et les approbations fondés sur les rôles, qui sont certifiés tous les trimestres, sont mis en œuvre dans tous les systèmes concernés de l'enquête afin d'appliquer le principe du moindre privilège.
6. Sécurité physique des emplacements où des renseignements personnels sont traités
   Les politiques et mesures de sécurité et de sûreté de PayPal à l'échelle internationale stipulent les exigences nécessaires pour faciliter l'application des mesures de sûreté et de sécurité efficaces, y compris la sécurité physique, conformément aux lois, règlements et exigences des partenaires applicables. Un accent

particulier est mis sur les systèmes de sécurité et les mesures de protection lors de la construction de zones spéciales ou sensibles telles que les salles de courrier, d'entreposage du matériel, les zones d'expédition et de réception, les salles informatiques/serveurs, les chambres fortes de communication ou les zones de stockage de documents classifiés ou d'informations conformément aux normes de sécurité des l'information de la Société.

7. Enregistrement et configuration des événements
   PayPal décrit et définit les types et les attributs d'enregistrement et de surveillance des événements. L'entreprise collecte et regroupe plusieurs types d'enregistrement vers le système de surveillance centralisé de la sécurité. Un contrôle standard de la gestion de la configuration est prévu pour s'assurer que les journaux sont collectés à partir des systèmes, puis transmis à notre système de surveillance centralisé de la sécurité. Les politiques de PayPal et les processus de soutien stipulent que les bases de configuration et renforcement de la sécurité doivent être mises en œuvre dans tous les systèmes.
8. Gouvernance et gestion des TI ; certification et assurance des processus et des produits
   PayPal promeut une philosophie de sécurité résiliente dans l’ensemble de l’entreprise. Notre responsable de la sécurité des informations supervise la sécurité des informations au sein de toute notre entreprise. Dans le cadre de notre programme de gestion des risques et de la conformité, notre programme de supervision technologique et de sécurité de l'information est conçu pour aider l'entreprise à gérer les risques liés à la technologie et à la sécurité de l'information, ainsi qu'à identifier, protéger, détecter, combattre et éliminer les menaces liées à la sécurité de l'information. PayPal certifie et assure ses processus et ses produits, par le truchement d’une gamme variée de programmes d'entreprise, y compris (i) des audits et des évaluations des obligations techniques standard de PayPal, y compris, mais sans s'y limiter, la norme ISO 27001, les normes applicables de l'industrie des paiements par carte (DSS, NIP, P2PE, etc.) et les normes SOC-1 et SOC-2 de l'American Institute of Certified Public Accountants (AICPA), (ii) le processus d'identification du contrôle des risques (RCIP) qui garantit un engagement rapide et une approche standard pour la mesure, la gestion et la surveillance des risques associés au développement et à la publication de solutions de produits, (iii) des évaluations

d'impact sur la vie privée qui sont intégrées aux premières étapes des processus de développement de produits et de logiciels, et (iv) un programme complet de gestion des tiers, qui fournit une assurance par la gestion continue des risques tout au long du cycle de vie d'un engagement avec un tiers.

9. Minimisation des données.
   Nos politiques exigent, par le biais de contrôles techniques, que les éléments de données collectés et générés soient adéquats, pertinents et limités à ce qui est nécessaire au regard des objectifs pour lesquels ils sont traités. Les processus d'évaluation des incidences sur la confidentialité de PayPal garantissent le respect de ces politiques.
10. Qualité et conservation des données
    La politique de gestion de l'accès et de la qualité de PayPal garantit que toutes les données personnelles sont correctes, complètes et à jour, et permet aux utilisateurs individuels d'accéder au système pour corriger et modifier leurs données (par exemple, leur adresse, leurs coordonnées, etc.) et, en cas de demande de correction de la part d'une personne concernée, de fournir un service qui réponde à son droit de correction. Notre programme de gouvernance des données prend en charge la qualité des données, les problèmes et les mesures correctives, le cas échéant. Nous exigeons que toutes les données soient classées en fonction de leur valeur commerciale et que des périodes de conservation leur soient attribuées, en fonction des exigences légales, réglementaires et commerciales de PayPal en matière d'archivage. À l'expiration de la période de conservation, les données et les informations sont retirées, supprimées ou détruites.
11. Responsabilité
    PayPal a mis au point un ensemble de politiques et de principes en matière de sécurité de l'information, de technologie, de gouvernance des données, de gestion des tiers et de confidentialité qui sont alignés sur les normes du secteur et conçus pour promouvoir la collaboration et le partenariat des parties prenantes dans la prise de conscience et le respect de ces politiques et contrôles au sein de l'organisation, afin d'assurer la participation et la responsabilité du sommet à la base de l'organisation. Chaque programme définit les responsabilités pour les décisions, les processus et les contrôles interfonctionnels liés aux données. En tant que responsable du traitement des données, PayPal est responsable et démontre sa conformité aux articles

pertinents portant une obligation de responsabilité dans le RGPD et d'autres lois sur la protection des données applicables par la mise en œuvre d'une politique de confidentialité et d'une structure de contrôle organisationnel et technique stratifiée sous-jacente pour assurer la conformité à l'échelle de l'entreprise avec la loi, la réglementation, la politique et les procédures de confidentialité. Celles-ci comprennent la capacité de démontrer la conformité aux lois sur la protection des données par le biais : 1) d'une solide culture de conformité, 2) d'une structure de gouvernance des risques et de la conformité de l'entreprise qui comprend des comités de gestion, des rôles de surveillance, des rapports sur la confidentialité, 3) de la responsabilité des fonctions commerciales en matière de conformité avec le programme de confidentialité, y compris l'établissement, la documentation et la maintenance des processus et des contrôles commerciaux, 4) d'un service international de gestion de la confidentialité au sein de l'organisation de la conformité de l'entreprise pour superviser la conformité de l'entreprise avec le programme de confidentialité et définir des politiques, des normes, des procédures et des outils qui sont opérationnalisés par les fonctions commerciales, 5) des communications avec l'entreprise par le service international de gestion de la confidentialité pour promouvoir la sensibilisation et la compréhension de la vie privée, 6) du cadre de gestion des risques et de la conformité de l'entreprise pour garantir l'utilisation de processus cohérents, notamment les évaluations des incidences sur la vie privée, la surveillance et les tests de confidentialité, la gestion des problèmes liés à la confidentialité, la formation à la gestion la confidentialité, le plan annuel de protection de la confidentialité, et 7) des rapports et analyses destinés aux comités de gestion qui supervisent le programme de protection de la vie privée.

12. Droits de la personne concernée
    PayPal a mis en place un programme visant à garantir le respect des droits des personnes concernées, notamment en matière d'accès, de correction et d'effacement. Les demandes d'effacement de données sont satisfaites à moins que PayPal n'ait une obligation légale ou réglementaire ou une autre raison commerciale légitime de les conserver. Les politiques de PayPal garantissent que l'effacement a lieu tout au long du cycle de vie du client.
13. Processeurs
    PayPal dispose d'un programme complet de gestion des tiers, qui

fournit une assurance par une gestion continue des risques tout au long du cycle de vie d'un engagement avec un tiers. Nous avons mis en place des contrôles contractuels pour exiger de nos processeurs et de leurs sous-processeurs qu'ils mettent en place des normes complètes de sécurité et de confidentialité des données tout au long de la chaîne de traitement. Tous les sous-processeurs doivent obtenir notre approbation préalable avant d'être engagés.

Protection des données : information d'enregistrement de l'importateur de données (le cas échéant)
Sans objet.

Informations complémentaires utiles (limites de stockage et autres informations pertinentes)
Selon les stipulations du Contrat la disposition ci-dessus de la présente Annexe 1.

Addenda antérieur sur la protection des données

Devient caduc le 1er novembre 2023

Le présent Addenda sur la protection des données (« Addenda ») est conclu entre le Marchand et PayPal (collectivement les « Parties »). Le présent Addenda fait partie du Contrat entre le Marchand et PayPal (le « Contrat ») conformément à la section « Effet du présent Addenda » ci-dessous.

Les termes en majuscules utilisés mais non définis dans le présent addenda ont le sens qui leur est conféré dans le Contrat.

I. EFFET DU PRÉSENT ADDENDA

Le présent addenda constitue une modification et une partie intégrante du Contrat. Il prend effet à la date d'entrée en vigueur du Contrat.

II. GÉNÉRALITÉS

1\. Définitions

Les termes ci-après ont les significations suivantes lorsqu'ils sont utilisés dans le présent Addenda :

-
  - a. « Contrat » désigne le Contrat de services ou le Contrat Marchand (selon le cas) conclu entre PayPal et le Marchand.
    b. Un « Contrôleur » (également appelé « responsable du traitement des données ») désigne une entité qui détermine les objectifs et les moyens du Traitement des données à caractère personnel. Si ce terme (ou un terme similaire ayant les mêmes fonctions) est déjà défini dans les Lois sur la protection des données en vigueur, le terme « Contrôleur », tel que mentionné dans les présentes, aura la signification prévue dans la Loi sur la protection des données applicable, y compris la signification d'une « Entreprise », le cas échéant, telle que définie dans la Loi californienne sur la protection de la vie privée des consommateurs de 2018.
    c. « Données du Marchand » désignent toutes les Données personnelles que PayPal reçoit du Marchand ou du Bénéficiaire relatives au Marchand, à un Bénéficiaire, ou liées à l'utilisation des Services Hyperwallet par le Marchand, existant avant ou après la date du présent Contrat.
    d. « Lois sur la protection des données » désignent toutes les lois, les réglementations, les directives, les exigences réglementaires et codes de pratique en matière de protection des données applicables à la fourniture des Services PayPal en vertu du présent Contrat, y compris toute modification de ceux-ci et toute réglementation ou tout instrument associé (exemple, qui pourrait inclure, sans s'y limiter, le Règlement général sur la protection des données (UE) 2016/679 (« RGPD »), la loi californienne sur la protection de la vie privée des consommateurs 2018, Cal. Civ. Code § 1798.100 et suivants (« CCPA »), et ses dispositions d'application, la Loi australienne de 1988 sur la protection de la vie privée (Cth), la loi sur la protection des renseignements personnels et les documents électroniques (Canada), l'Ordonnance sur les données personnelles (vie privée) (Cap.486) (Hong Kong), la Loi générale brésilienne sur la protection des données, la Loi Fédérale N° 13 709/2018, et la Loi sur la Protection des Données Personnelles 2012

(Singapour)).
e. « PayPal Group » désigne PayPal, Inc. et toutes les sociétés que PayPal, ou son/ses successeur(s), possède ou contrôle directement ou indirectement.
f. « Bénéficiaire » désigne une personne ou une entreprise recevant un paiement par le biais des Services Hyperwallet utilisés par le Marchand.
g « Une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment au moyen d'un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou au moyen d'un ou plusieurs éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique.
h. Les termes « Traitement » ou « traité » ou « en cours de traitement » désignent : toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, y compris la collecte, l'enregistrement, la conservation, le partage, l'organisation, le stockage, l'accès, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, la divulgation, la diffusion, la mise à disposition, l'alignement, la combinaison, le blocage, la suppression, la suppression ou la destruction.

2. PayPal comme contrôleur?
PayPal doit se conformer aux exigences des lois sur la protection des données applicables aux contrôleurs en ce qui concerne l'utilisation des Données du Marchand (y compris, sans s'y limiter, la mise en œuvre et l'application en permanence toutes les mesures de sécurité appropriées relatives au traitement des données du Marchand) et ne doit rien faire, ni autoriser sciemment une action susceptible d'exposer le marchand à une violation des Lois sur la protection des données. PayPal ne transfère les Données du Marchand qu'à des tiers, des sous-traitants ou des membres du Groupe PayPal qui signent des accords écrits stipulant les conditions de protection des Données du Marchand au moins aussi explicites que les conditions énoncées dans le présent Addenda. Dans le cas où le Marchand choisit une solution de paiement où un bénéficiaire n'est pas tenu d'ouvrir un compte via la solution hébergée par Hyperwallet, le Marchand accepte de présenter la politique de confidentialité d'Hyperwallet (https://pay.hyperwallet.com/hw2web/consumer/page/privacyAgreemen

t.xhtml) à ses bénéficiaires avant de partager les données personnelles de ses bénéficiaires avec PayPal.

3. Traitement des données du marchand dans le cadre des Services Hyperwallet
Les Parties reconnaissent et acceptent que lorsque PayPal fournit des Services Hyperwallet au Marchand, ce dernier et PayPal sont tous deux des Contrôleurs indépendants pour toutes les Données du Marchand traitées dans le cadre des Services Hyperwallet. À ce titre, PayPal détermine indépendamment l'objectif et les moyens du traitement de ces Données marchandes et ne constitue pas un contrôleur conjoint avec le Marchand en ce qui concerne les données du Marchand. Les Parties reconnaissent et acceptent que PayPal peut utiliser, reproduire et traiter les Données du Marchand et les données relatives aux transactions de paiement pour les raisons précises suivantes :

- a. Selon que cela est raisonnablement nécessaire, pour fournir et améliorer les Services Hyperwallet destinés au Marchand et à ses Bénéficiaires, y compris les outils de protection contre la fraude ;
  b. Pour surveiller, prévenir et détecter les transactions de paiement frauduleuses, et pour éviter tout préjudice au Marchand, à PayPal et à des tiers ;
  c. Pour se conformer aux obligations légales ou réglementaires applicables au Traitement et à la conservation des données de paiement auxquelles PayPal est soumis, y compris les obligations applicables en matière de lutte contre le blanchiment d'argent et de vérification d'identité ;
  d. Pour analyser, développer et améliorer les produits et services de PayPal ;
  e. Pour une utilisation interne, y compris, entre autres, pour l'analyse des données et les mesures;
  f. Pour compiler et divulguer les Données du Marchand et les données sur les transactions de paiement dans leur ensemble lorsque les Données personnelles ou les données d'utilisateur du Marchand ne sont pas identifiables, y compris le calcul des moyennes du Marchand par région ou par secteur ;
  g. Pour se conformer aux exigences légales applicables et aider les organismes chargés de l'application de la loi en répondant aux demandes de divulgation d'informations conformément aux lois ; et
  h. Pour toute autre raison pour laquelle PayPal notifie le Marchand,

à condition que cette raison soit conforme aux Lois sur la protection des données en vigueur.

4. Assistance mutuelle

Les parties conviennent de coopérer l'une avec l'autre selon les besoins pour permettre à l'autre partie de s'acquitter convenablement de sa responsabilité en tant que Contrôleur indépendant en vertu des Lois sur la protection des données. Les parties conviennent que, dans la mesure où le Marchand reçoit une demande d'accès d'un bénéficiaire ou si un bénéficiaire se prévaut de ses droits en vertu des lois sur la protection des données, le Marchand doit répondre directement à la demande d'accès de ce bénéficiaire. Le Marchand doit également informer les Bénéficiaires qu'ils peuvent exercer leurs droits en matière de données liées aux Services Hyperwallet auprès de PayPal conformément aux instructions de la Déclaration de confidentialité disponible à l'adresse https://www.hyperwallet.com/privacy-policy/ (qui peut être modifiée de temps à autre). En outre, si dans le cadre d'un incident de sécurité, PayPal détermine à sa discrétion qu'il doit notifier les bénéficiaires concernés, et qu'il ne dispose pas de toutes coordonnées de ces bénéficiaires pour effectuer cette communication, le Marchand doit alors s'efforcer de fournir à PayPal les informations dont il dispose sur ce Bénéficiaire dans le seul but de permettre à PayPal de se conformer aux obligations de notification applicables aux bénéficiaires concernés en vertu de la Loi sur la protection des données.

5. Partage transfrontalier des données

Les parties conviennent que PayPal peut transférer les données du marchand traitées en vertu du présent Contrat en dehors du pays où elles ont été collectées si nécessaire pour fournir les Services Hyperwallet. Si PayPal transfère des données du marchand protégées par la présente Annexe vers une juridiction pour laquelle l'autorité de réglementation compétente du pays dans lequel les données ont été collectées n'a pas émis de décision de conformité (une « Décision de conformité »), PayPal s'assurera que des mesures de protection appropriées ont été mises en œuvre pour le transfert des Données du Marchand conformément aux Lois sur la protection des données en vigueur. Pour se conformer au RGPD, PayPal s'appuie par exemple sur des règles d'entreprise contraignantes approuvées par les autorités de contrôle compétentes et sur d'autres mécanismes de transfert de données pour les transferts de données des Marchands à d'autres membres du groupe PayPal.

-
  -
    - a. En ce qui concerne les transferts de données à un membre du Groupe PayPal se trouvant dans un pays qui ne bénéficie pas d’une décision de conformité des Bénéficiaires résidant dans l'Union européenne, en Suisse, dans l'Espace économique européen, et/ou dans leurs États membres et au Royaume-Uni, les Parties conviennent (i) dans la mesure où cela s'applique, votre signature du Contrat sera considérée comme une signature et une acceptation de la Décision d'exécution (UE) 2021/914 de la Commission européenne du 4 juin 2021 relative aux clauses contractuelles standard pour le transfert de données à caractère personnel vers des pays tiers conformément au RGPD (« Clauses de transfert de l'UE ») par le Marchand, en tant qu'exportateur de données et dans le rôle de contrôleur, et sera considéré comme une signature et une acceptation des clauses de protection de données standard spécifiées dans les règlements établis par le Secrétaire d'État en vertu de la section 17C(b) de la Loi sur la protection des données de 2018 et, à ce jour, en vigueur au Royaume-Uni (les « Clauses de transfert du Royaume-Uni »), en tant qu'exportateur de données (ii) dans la mesure où elles s'appliquent, la signature du Contrat par le membre du Groupe PayPal sera considérée comme une signature et une acceptation des Clauses de transfert de l'UE par ce membre du Groupe PayPal, en tant qu'importateur de données et en tant que responsable du traitement, et sera considérée comme une signature et une acceptation des Clauses de transfert du Royaume-Uni, en tant qu'importateur de données ; et (iii) les parties seront soumises aux dispositions du Module 1 des Clauses de transfert de l'UE. Si la Commission européenne ou le Secrétaire d'État britannique (ou tout autre organisme britannique autorisé) révise et publie ensuite de nouvelles Clauses de transfert de l'UE

ou Clauses de transfert du Royaume-Uni, selon le cas (ou si la Commission européenne ou le Secrétaire d'État britannique (ou tout autre organisme britannique autorisé) l'exige ou l'applique), les parties conviennent que ces nouvelles clauses de transfert de l'UE ou clauses de transfert du Royaume-Uni, selon le cas, remplaceront les présentes clauses de transfert de l'UE ou clauses de transfert du Royaume-Uni, selon le cas, et elles acceptent de prendre toutes les mesures nécessaires à la mise en œuvre de ces nouvelles clauses de transfert, selon le cas. Les Clauses de transfert de l'UE (module 1) et les Clauses de transfert du Royaume-Uni seront toutes deux incorporées dans l'accord par renvoi et considérées comme dûment exécutées entre les parties lors de l'entrée en vigueur du présent Contrat, sous réserve des précisions suivantes :

A) Clauses de transfert de l'UE

1. L’option 1 de la clause 17 (loi applicable) s’applique et les lois luxembourgeoises régissent les clauses de l'UE ;
2. Conformément à la clause 18 (Choix du forum et de la juridiction), les tribunaux luxembourgeois résoudront tout litige découlant des clauses de l’UE ; et
3. Les parties conviennent que les détails requis en vertu de l'Annexe sur les clauses de transfert de l'UE sont indiqués dans la pièce jointe 1.

B) Clauses de transfert du Royaume-Uni

1. La clause II(h)(iii) est incorporée et la signature du Contrat par PayPal sera considérée comme le paraphe requis de PayPal en tant qu'importateur de données ;
2. Les parties conviennent que les détails requis en vertu de l’annexe B des Clauses de transfert du Royaume-Uni sont indiqués dans la pièce jointe 1 (dans la mesure du possible).

<u>Pièce jointe 1</u>

<u>Annexe aux Clauses de transfert de l’UE et Annexe B des Clauses de transfert du Royaume-Uni</u>

A) Les éléments suivants sont applicables, dans la mesure requise, en vertu des Clauses de transfert de l'UE et des Clauses de transfert du Royaume-Uni

Annexe 1.A. Liste des Parties

Exportateur de données

- Nom et adresse : Nom et adresse : l'exportateur de données est le Marchand et l'adresse est celle indiquée dans le Contrat
- Nom, fonction et coordonnées de la personne-ressource : tels que prévus dans le Contrat
- Activités relatives aux données transférées en vertu de la Clause contractuelle standard: comme prévu dans le Contrat
- Signature et date : veuillez consulter la section « Transferts transfrontaliers » du présent Addenda.
- Rôle (Contrôleur/processeur) : contrôleur

Importateur de données

- Nom et adresse : L'importateur de données est le membre du groupe PayPal qui fournit les services conformément au Contrat et son adresse est celle indiquée dans le Contrat.
- Nom, fonction et coordonnées de la personne-ressource : tels que prévus dans le Contrat
- Activités pertinentes pour les données transférées en vertu de la clause contractuelle standard : comme prévu dans le Contrat. Signature et date : veuillez consulter la section « Transferts transfrontaliers » du présent Addenda.
- Rôle (Contrôleur/processeur) : contrôleur

Annexe 1.B. Description du transfert

Personnes concernées dont les Données personnelles sont transférées
Les données personnelles transférées se rapportent aux catégories de personnes concernées suivantes :

- Les clients, les employés et les autres contacts professionnels de l'exportateur de données.

Catégories de données personnelles transférées
Les données personnelles transférées peuvent contenir les catégories de données suivantes :

- Le nom du Marchand et du bénéficiaire, le montant de la transaction, la date et l'heure, les coordonnées du compte bancaire, les détails de la carte de paiement, le cryptogramme visuel, le code postal, le code du pays, l'adresse, l'adresse de courriel, le télécopieur, le numéro de téléphone, le site Web, les données d'expiration, les données d'expédition, le statut fiscal, l'identifiant unique du client, l'adresse IP, la localisation, les informations sur les représentants du client, les informations sur la propriété bénéficiaire, les détails commerciaux et d'autres informations requises pour la connaissance du client et toutes les autres données reçues par PayPal en vertu du Contrat.

Transfert de données sensibles (le cas échéant) et restrictions ou mesures de protection appliquées
Les données personnelles transférées concernent les catégories de données sensibles suivantes :

- Sans objet, sauf si le marchand configure le service pour collecter ces données.

Applique des restrictions et des mesures de protection :

- Sans objet, sauf si le marchand configure le service pour collecter ces données.

Nature du traitement
Tel qu'énoncé dans le Contrat.

Objectif(s) du/des transfert(s)
Le transfert est effectué aux fins suivantes :

- Exécuter les services fournis par l'importateur de données à l'exportateur de données conformément au Contrat.
- Identifier les activités frauduleuses et les risques affectant ou susceptibles d'affecter l'importateur de données, l'exportateur de données ou d'autres clients de l'importateur de données.
- Respecter les lois applicables à l’importateur de données.
- Tel qu’indiqué dans l’Addenda sur la protection des données

Durée de conservation des données à caractère personnel ou, si cela n'est pas possible, critères utilisés pour déterminer cette durée.
L'importateur de données ne conserve les données à caractère

personnel qu'aussi longtemps que nécessaire compte tenu du but ou des buts pour lesquels elles ont été collectées (voir les buts ci-dessus). Pour déterminer la durée de conservation appropriée des données à caractère personnel, l'importateur de données tient compte de la quantité, de la nature et de la sensibilité des données à caractère personnel, du risque potentiel de dommage résultant d'une utilisation ou d'une divulgation non autorisée de celles-ci, des fins pour lesquelles les données à caractère personnel sont traitées et de la possibilité d'atteindre ces objectifs par d'autres moyens, ainsi que des exigences légales, réglementaires, fiscales, comptables ou autres qui s'appliquent.

Pour les transferts vers des (sous-)processeurs, précisez également l’objet, la nature et la durée du traitement
L'importateur de données peut partager des données à caractère personnel avec des prestataires de services tiers qui fournissent des services et exercent des fonctions selon les instructions de l'importateur de données et en son nom. Ces fournisseurs de services tiers peuvent, par exemple, fournir un élément des Services proposés dans le cadre du Contrat, comme le Service vérification client, le traitement des transactions ou le Service clientèle, ou fournir un service à l’importateur de renseignements qui prend en charge les Services fournis dans le cadre du Contrat, comme le stockage. Lorsqu’il détermine la durée du traitement effectué par les fournisseurs de services tiers, l’importateur de données applique les critères indiqués ci-dessus dans la présente Annexe I.B.

Annexe 1.C. Autorité de surveillance
Conformément à la Clause 13(a) des Clauses de transfert de l'UE, l'autorité de surveillance responsable de la conformité de l'exportateur de données avec le règlement (UE) 2016/679 en ce qui concerne le transfert de données, comme indiqué, agira en tant qu'autorité de surveillance compétente.

Annexe II Mesures techniques et organisationnelles Il s’agit de mesures techniques et organisationnelles visant à assurer la sécurité des données

1. Pseudonymisation, cryptage et protection des données lors de leur transmission.
   Les politiques de PayPal garantissent le respect de ce principe et exigent l'utilisation de contrôles techniques pour prévenir le risque

de divulgation des données personnelles. PayPal utilise le cryptage en transit et au repos pour toutes les données personnelles. Nous utilisons également des techniques de pseudonymisation standard de l'industrie, telles que la création de jetons, pour protéger les données personnelles, le cas échéant. PayPal dispose de politiques complètes qui prévoient des obligations et des processus clés pour protéger les données lorsqu'elles sont transférées au sein de l'entreprise et à l'extérieur avec des tiers.

2. Gestion du changement et continuité des activités
   Le processus de gestion des changements de PayPal protège la disponibilité et la résilience des données et des systèmes pendant tout leur cycle de vie en s'assurant que les changements sont planifiés, approuvés, exécutés et revus de manière appropriée. Le processus de gestion de la continuité des activités de l'entreprise fournit un cadre permettant de renforcer la résilience de l'organisation et d'apporter une réponse efficace qui préserve les intérêts de ses principales parties prenantes.
3. Reprise après sinistre.
   Le programme résilient de reprise après sinistre de PayPal prévoit des processus de récupération des informations ou des systèmes technologiques en cas de perturbation importante, en mettant l'accent sur les systèmes informatiques qui soutiennent les processus commerciaux essentiels et les activités des clients. Les infrastructures technologiques de PayPal sont hébergées dans plusieurs centres de données sécurisés, avec des fonctionnalités principales et secondaires, chacun étant équipé d'une infrastructure de réseau et de sécurité, de serveurs d'applications et de bases de données dédiés et d'un espace de stockage.
4. Test, inspection et évaluation réguliers de l'efficacité des mesures techniques et organisationnelles
   PayPal planifie, exécute et communique régulièrement les résultats du programme de test de la société afin d'évaluer l'efficacité de ses mesures technologiques et organisationnelles. Le programme est géré par notre équipe chargée des risques d'entreprise et de la conformité, qui collabore avec les parties prenantes concernées pour obtenir et évaluer les informations requises pour les tests, les rapports et les mesures correctives nécessaires.
5. Identification et autorisation de l'utilisateur.
   Les processus de gestion des accès de PayPal exigent que les utilisateurs se connectent au réseau de l'entreprise à l'aide d'un Identifiant de compte du réseau d'entreprise unique et d'un mot

de passe pour l'identification et l'authentification de l'utilisateur avant d'accéder à toute autre application concernée. Des politiques automatisées concernant la composition, la longueur, la modification, la réutilisation et le verrouillage des mots de passe sont appliquées. L'accès et les approbations fondés sur les rôles, qui sont certifiés tous les trimestres, sont mis en œuvre dans tous les systèmes concernés de l'enquête afin d'appliquer le principe du moindre privilège.

6. Sécurité physique des emplacements où des renseignements personnels sont traités
   Les politiques et mesures de sécurité et de sûreté de PayPal à l'échelle internationale stipulent les exigences nécessaires pour faciliter l'application des mesures de sûreté et de sécurité efficaces, y compris la sécurité physique, conformément aux lois, règlements et exigences des partenaires applicables. Un accent particulier est mis sur les systèmes de sécurité et les mesures de protection lors de la construction de zones spéciales ou sensibles telles que les salles de courrier, d'entreposage du matériel, les zones d'expédition et de réception, les salles informatiques/serveurs, les chambres fortes de communication ou les zones de stockage de documents classifiés ou d'informations conformément aux normes de sécurité des l'information de la Société.
7. Enregistrement et configuration des événements
   PayPal décrit et définit les types et les attributs d'enregistrement et de surveillance des événements. L'entreprise collecte et regroupe plusieurs types d'enregistrement vers le système de surveillance centralisé de la sécurité. Un contrôle standard de la gestion de la configuration est prévu pour s'assurer que les journaux sont collectés à partir des systèmes, puis transmis à notre système de surveillance centralisé de la sécurité. Les politiques de PayPal et les processus de soutien stipulent que les bases de configuration et renforcement de la sécurité doivent être mises en œuvre dans tous les systèmes.
8. Gouvernance et gestion des TI ; certification et assurance des processus et des produits
   PayPal promeut une philosophie de sécurité résiliente dans l'ensemble de l'entreprise. Notre responsable de la sécurité des informations supervise la sécurité des informations au sein de toute notre entreprise. Dans le cadre de notre programme de gestion des risques et de la conformité, notre programme de supervision technologique et de sécurité de l'information est

conçu pour aider l'entreprise à gérer les risques liés à la technologie et à la sécurité de l'information, ainsi qu'à identifier, protéger, détecter, combattre et éliminer les menaces liées à la sécurité de l'information. PayPal certifie et assure ses processus et ses produits, par le truchement d'une gamme variée de programmes d'entreprise, y compris (i) des audits et des évaluations des obligations techniques standard de PayPal, y compris, mais sans s'y limiter, la norme ISO 27001, les normes applicables de l'industrie des paiements par carte (DSS, NIP, P2PE, etc.) et les normes SOC-1 et SOC-2 de l'American Institute of Certified Public Accountants (AICPA), (ii) le processus d'identification du contrôle des risques (RCIP) qui garantit un engagement rapide et une approche standard pour la mesure, la gestion et la surveillance des risques associés au développement et à la publication de solutions de produits, (iii) des évaluations d'impact sur la vie privée qui sont intégrées aux premières étapes des processus de développement de produits et de logiciels, et (iv) un programme complet de gestion des tiers, qui fournit une assurance par la gestion continue des risques tout au long du cycle de vie d'un engagement avec un tiers.

9. Minimisation des données.
   Nos politiques exigent, par le biais de contrôles techniques, que les éléments de données collectés et générés soient adéquats, pertinents et limités à ce qui est nécessaire au regard des objectifs pour lesquels ils sont traités. Les processus d'évaluation des incidences sur la confidentialité de PayPal garantissent le respect de ces politiques.
10. Qualité et conservation des données
    La politique de gestion de l'accès et de la qualité de PayPal garantit que toutes les données personnelles sont correctes, complètes et à jour, et permet aux utilisateurs individuels d'accéder au système pour corriger et modifier leurs données (par exemple, leur adresse, leurs coordonnées, etc.) et, en cas de demande de correction de la part d'une personne concernée, de fournir un service qui réponde à son droit de correction. Notre programme de gouvernance des données prend en charge la qualité des données, les problèmes et les mesures correctives, le cas échéant. Nous exigeons que toutes les données soient classées en fonction de leur valeur commerciale et que des périodes de conservation leur soient attribuées, en fonction des exigences légales, réglementaires et commerciales de PayPal en matière d'archivage. À l'expiration de la période de conservation,

les données et les informations sont retirées, supprimées ou détruites.

11. Responsabilité
    PayPal a mis au point un ensemble de politiques et de principes en matière de sécurité de l'information, de technologie, de gouvernance des données, de gestion des tiers et de confidentialité qui sont alignés sur les normes du secteur et conçus pour promouvoir la collaboration et le partenariat des parties prenantes dans la prise de conscience et le respect de ces politiques et contrôles au sein de l'organisation, afin d'assurer la participation et la responsabilité du sommet à la base de l'organisation. Chaque programme définit les responsabilités pour les décisions, les processus et les contrôles interfonctionnels liés aux données. En tant que responsable du traitement des données, PayPal est responsable et démontre sa conformité aux articles pertinents portant une obligation de responsabilité dans le RGPD et d'autres lois sur la protection des données applicables par la mise en œuvre d'une politique de confidentialité et d'une structure de contrôle organisationnel et technique stratifiée sous-jacente pour assurer la conformité à l'échelle de l'entreprise avec la loi, la réglementation, la politique et les procédures de confidentialité. Celles-ci comprennent la capacité de démontrer la conformité aux lois sur la protection des données par le biais : 1) d'une solide culture de conformité, 2) d'une structure de gouvernance des risques et de la conformité de l'entreprise qui comprend des comités de gestion, des rôles de surveillance, des rapports sur la confidentialité, 3) de la responsabilité des fonctions commerciales en matière de conformité avec le programme de confidentialité, y compris l'établissement, la documentation et la maintenance des processus et des contrôles commerciaux, 4) d'un service international de gestion de la confidentialité au sein de l'organisation de la conformité de l'entreprise pour superviser la conformité de l'entreprise avec le programme de confidentialité et définir des politiques, des normes, des procédures et des outils qui sont opérationnalisés par les fonctions commerciales, 5) des communications avec l'entreprise par le service international de gestion de la confidentialité pour promouvoir la sensibilisation et la compréhension de la vie privée, 6) du cadre de gestion des risques et de la conformité de l'entreprise pour garantir l'utilisation de processus cohérents, notamment les évaluations des incidences sur la vie privée, la surveillance et les tests de confidentialité, la gestion des problèmes liés à la confidentialité, la

formation à la gestion la confidentialité, le plan annuel de protection de la confidentialité, et 7) des rapports et analyses destinés aux comités de gestion qui supervisent le programme de protection de la vie privée.

12. Droits de la personne concernée
    PayPal a mis en place un programme visant à garantir le respect des droits des personnes concernées, notamment en matière d'accès, de correction et d'effacement. Les demandes d'effacement de données sont satisfaites à moins que PayPal n'ait une obligation légale ou réglementaire ou une autre raison commerciale légitime de les conserver. Les politiques de PayPal garantissent que l'effacement a lieu tout au long du cycle de vie du client.
13. Processeurs
    PayPal dispose d'un programme complet de gestion des tiers, qui fournit une assurance par une gestion continue des risques tout au long du cycle de vie d'un engagement avec un tiers. Nous avons mis en place des contrôles contractuels pour exiger de nos processeurs et de leurs sous-processeurs qu'ils mettent en place des normes complètes de sécurité et de confidentialité des données tout au long de la chaîne de traitement. Tous les sous-processeurs doivent obtenir notre approbation préalable avant d'être engagés.

B) Les éléments suivants s'appliquent uniquement aux destinataires des clauses de transfert du Royaume-Uni
Les données personnelles transférées ne pourront être divulguées qu'aux destinataires suivants :

- Les fournisseurs de services de l'importateur de données (comme indiqué ci-dessus), les filiales et le personnel fournissant des services conformément au Contrat.

Protection des données : information d'enregistrement de l'importateur de données (le cas échéant)
Sans objet.

Informations complémentaires utiles (limites de stockage et autres informations pertinentes)
Selon les stipulations du Contrat la disposition ci-dessus de la présente Annexe 1.