

[\*\*>> Afficher tous les contrats d'utilisation\*\*](#)

## Addenda PayPal sur la protection des données pour les produits de traitement de cartes

Dernière mise à jour : 10 décembre 2021

Le présent Addenda sur la protection des données de PayPal pour l'Addenda sur les produits de traitement des cartes (le présent « Addenda ») s'applique à tout produit, service ou autre offre dans lesquels un membre du groupe PayPal (« PayPal ») fournit des services de traitement de cartes, de passerelles et/ou de services de protection contre la fraude (les « Services de paiement ») à vous, le Marchand (le « Marchand » ou « Vous »). Le présent Addenda ne s'applique pas aux services de portefeuille PayPal tels que Payer avec PayPal ou les offres de paiement ultérieur de PayPal. Le présent Addenda fait partie du contrat pertinent entre le Marchand et PayPal qui régit la fourniture par PayPal des services de paiement à votre égard (le « Contrat ») et est intégré par référence dans celui-ci. En cas de conflit entre les modalités de cet Addenda et du Contrat, les modalités de l'Addenda prévaudront. Les termes en majuscules utilisés, mais non définis dans le présent Addenda, ont la signification énoncée dans le Contrat.

Le présent Addenda entrera en vigueur à la fin de (i) la date d'entrée en vigueur indiquée dans le Contrat ou (ii) la date d'entrée en vigueur indiquée dans l'avis affiché ou qui vous est fourni dans le cadre du présent Addenda. Nous pouvons modifier cet Addenda de temps à autre. La version révisée entrera en vigueur à la date de sa publication sur notre site Web, sauf en cas d'indication contraire. Si nos modifications réduisent vos droits ou accroissent vos responsabilités, nous publierons un avis sur la page « Mises à jour des politiques » de notre site Web dans les délais requis par le Contrat. Si vous n'acceptez pas les modifications apportées à cet Addenda, vous pouvez cesser d'utiliser les services de paiement.

### Définitions

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

L'expression «**Responsable du traitement** » désigne une entité qui détermine les finalités et les moyens du traitement des données personnelles ou, si cette expression (ou des conditions traitant des fonctions similaires) est définie dans la loi sur la protection des données, l'expression « Responsable du traitement » s'entend au sens de la loi sur la protection des données applicable.

Le terme «**Client**» désigne vos clients qui utilisent les services de paiement et aux fins du présent Addenda, sont des personnes concernées.

«**Données du client**» désigne les données personnelles que (i) le client fournit au marchand et au marchand et transmet à PayPal par l'intermédiaire de l'utilisation par le marchand des services de paiement et (ii) PayPal peut recueillir de l'appareil et du navigateur du client par l'intermédiaire d'un marchand de services de paiement.

«**Loi sur la protection des données** » désigne toutes les lois, réglementations, directives, exigences réglementaires et codes de pratiques applicables en matière de protection des données applicables à la fourniture des services de paiement, y compris les modifications y afférentes, ainsi que tout règlement ou tout instrument associé (p. ex., loi de Californie sur la protection des consommateurs 2018, Cal. Civ. Code § 1798,100 et suiv., règlement général sur la protection des données (UE) 2016/679 (GDPR), la loi australienne sur la confidentialité 1988 (CTH), la loi sur la protection des renseignements personnels et les documents électroniques (Canada), l'ordonnance sur la protection des données personnelles (chap. 486). (Hong Kong), la loi brésilienne générale sur la protection des données, loi fédérale n ° 13 709/2018 et la loi sur la protection des données personnelles 2012 (Singapour)).

« **Groupe PayPal** » désigne PayPal, Inc. et toutes les sociétés dans lesquelles PayPal ou son successeur, directement ou indirectement, détient ou contrôle de temps à autre.

« **Données personnelles** » désigne toute information relative à une personne physique identifiée ou identifiable (une « personne concernée »); une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, en particulier par référence à un identificateur, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou un ou plusieurs facteurs propres à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique.

Les « **processus** » ou les termes traitant de fonctions similaires lorsqu'ils sont utilisés dans le présent Addenda ont la signification définie dans les lois applicables sur la protection des données.

### **PayPal en tant que responsable du traitement**

PayPal se conformera aux exigences des lois sur la protection des données applicables aux Responsables du traitement en ce qui concerne le traitement des Données Client en vertu de la présente annexe (y compris, sans s'y limiter, en mettant en œuvre et en maintenant à tout moment toutes les mesures de sécurité appropriées en ce qui concerne le traitement des Données Client) et ne fera pas sciemment quelque chose ou ne permettra pas que quelque chose soit fait en ce qui concerne les Données Client qui conduirait probablement à une violation par le Marchand des lois sur la protection des données. PayPal ne transférera les données du client qu'à des tiers, des sous-processeurs ou des membres du groupe PayPal qui signeront des contrats écrits qui contiennent des conditions pour la protection des Données Client, qui ne sont pas moins protectrices que les conditions énoncées dans le présent addendum.

### **Traitement des données des clients dans le cadre des services de paiement**

Les parties reconnaissent et conviennent que le marchand et le PayPal sont tous des contrôleurs indépendants en ce qui concerne toutes les données de client traitées dans le cadre des services de paiement. En tant que tel, PayPal détermine indépendamment le motif et les moyens du traitement de ces données de client et n'est pas un contrôleur conjoint du marchand en ce qui concerne ces données de client.

Les parties reconnaissent et acceptent que PayPal est autorisé à utiliser, à reproduire et à traiter les Données des clients et les données des transactions de paiement aux fins restreintes suivantes :

- comme cela est raisonnablement nécessaire pour fournir et améliorer les services de paiement au marchand et à ses clients, y compris les outils de protection contre la fraude ;
- Afin de surveiller, de prévenir et de détecter les transactions de paiement frauduleuses et de prévenir les dommages au Marchand, à PayPal et à des tiers,
- Pour se conformer aux obligations légales ou réglementaires applicables au traitement et à la conservation des données de paiement dont PayPal est l'objet, y compris les obligations en matière de lutte contre le blanchiment d'argent et la vérification de l'identité;
- Pour analyser, développer et améliorer les produits et les services de PayPal;

- Pour utilisation interne, y compris, notamment, l'analytique et les métriques des données;
- compiler et divulguer les données des clients et les données de la transaction de paiement au cours de l'agrégat où les données de vos clients particuliers ou utilisateurs ne sont pas identifiables, y compris le calcul de vos moyennes par région ou par secteur d'activité ;
- Pour se conformer aux exigences légales en vigueur et pour aider les organismes d'application de la loi en répondant aux demandes de divulgation de renseignements conformément aux lois; et
- À toute autre fin dont avis est donné au Marchand, pourvu que cette fin soit conforme aux lois sur la protection des données.

## **Avis du Marchand aux Clients**

Le Marchand doit faire des efforts commercialement raisonnables pour (i) informer les clients dans leur politique de confidentialité que PayPal est un Responsable du traitement indépendant aux fins du traitement des Données Client décrite dans le présent Addenda et (ii) inclure un lien vers la déclaration de confidentialité de PayPal disponible sur [www.paypal.com](http://www.paypal.com) dans la politique de confidentialité du Marchand.

## **Assistance mutuelle**

Les parties acceptent de collaborer dans la mesure raisonnablement nécessaire afin de permettre à l'autre partie de s'acquitter convenablement de sa responsabilité de Responsable du traitement 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 Client en vertu des lois sur la protection des données, le Marchand doit répondre directement à la demande d'accès du Client. Le Marchand doit également informer le Client qu'il peut exercer ses droits sur la personne concernée dans le cadre des services de paiement avec PayPal conformément aux instructions décrites dans la déclaration de confidentialité disponible sur le site [www.paypal.com](http://www.paypal.com). De plus, en cas d'incident de sécurité, si PayPal détermine à son entière discrétion qu'elle doit aviser les Clients touchés et que PayPal ne dispose pas des coordonnées nécessaires pour communiquer avec un Client touché, alors le Marchand déploiera les efforts commercialement raisonnables pour fournir à PayPal les coordonnées qu'il possède sur le Client aux fins restreintes de permettre à PayPal de s'acquitter de ses obligations légales à l'égard du Client touché en vertu des lois sur la protection des données.

## **Transmission de données transfrontalières**

Les parties conviennent que PayPal peut transférer les données des clients traitées en vertu du présent contrat à l'extérieur du pays où elle a été collectée, au besoin, pour fournir les services de paiement. Si PayPal transfère les données des clients protégées en vertu du présent Addenda à une juridiction pour laquelle l'autorité de réglementation applicable au pays dans lequel les données ont été collectées n'a pas émis de décision d'adéquation, PayPal veillera à ce que des mesures de protection appropriées aient été mises en œuvre pour le transfert de données de clients conformément aux lois applicables en matière de protection des données. Par exemple, et à des fins de conformité avec le RGPD, nous nous appuyons sur des règles d'entreprise contraignantes approuvées par les autorités de surveillance compétentes et d'autres mécanismes de transfert de données pour les transferts de données de clients vers d'autres membres du groupe de PayPal.

En ce qui concerne vos transferts de données vers PayPal de vos clients situés dans l'Union européenne, en Suisse, dans l'Espace économique européen et/ou dans leurs États membres ou le Royaume-Uni, nous convenons chacun que (i) dans la mesure du possible, votre signature du Contrat sera considéré comme la signature et l'acceptation de la Décision d'exécution (UE) 2021/914 de la Commission européenne du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du RGPD (« Clauses de transfert de l'UE ») par le Marchand, en tant qu'exportateur de données et dans le rôle de responsable du traitement, et sera considéré comme la signature et l'acceptation des clauses types de protection des données spécifiées dans les règlements pris par le Secrétaire d'État en vertu de l'article 17C(b) de la loi sur la protection des données de 2018 et pour l'instant, en vigueur au Royaume-Uni (les « Clauses de transfert du Royaume-Uni »), en tant qu'exportateur de données (ii) dans la mesure applicable, la signature du Contrat par PayPal sera considérée comme la signature et l'acceptation des Clauses de transfert de l'UE par PayPal, en tant qu'importateur de données et en tant que responsable du traitement, et sera considéré comme la signature et l'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. Dans l'éventualité où la Commission européenne ou le Secrétaire d'État du Royaume-Uni (ou tout autre organisme britannique autorisé) révise et publie par la suite de nouvelles Clauses de transfert de l'UE, respectivement (ou tel que requis ou mis en œuvre par la Commission européenne ou le Secrétaire d'État du Royaume-Uni (ou tout autre organisme britannique autorisé)), 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 les Clauses de transfert du Royaume-Uni, selon le cas, et que les parties conviennent de prendre toutes les mesures nécessaires pour effectuer l'exécution des nouvelles

Clauses de transfert de l'UE ou des Clauses de transfert du Royaume-Uni, selon le cas. Les Clauses de transfert de l'UE (Module 1) et les Clauses de transfert du Royaume-Uni seront incorporées dans le Contrat par référence et seront considérées comme dûment exécutées entre les parties après l'entrée en vigueur du présent Contrat sous réserve des détails suivants :

A) Clauses de transfert de l'UE

1. l'option 1 de la clause 17 (loi applicable) s'applique et les lois luxembourgeoise 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 exigés 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).

**Pièce jointe 1**

**Annexe aux Clauses de transfert de l'UE et annexe B des Clauses de transfert du Royaume-Uni**

**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**

**Exportateur de données**

- 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 : comme prévu dans le contrat
- Activités relatives aux données transférées en vertu de la Clause contractuelle type : comme prévu dans le contrat
- Signature et date : veuillez consulter la section « Transferts transfrontaliers » du présent Addenda
- Rôle (responsable du traitement/processeur) : responsable du traitement

## **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 : comme prévu dans le contrat
- Activités pertinentes pour les données transférées en vertu de la clause contractuelle type : comme prévu dans le Contrat Signature et date : veuillez consulter la section « Transferts transfrontaliers » du présent Addenda.
- Rôle (responsable du traitement/processeur) : responsable du traitement

## **Annexe 1.B. Description du transfert**

### **Personnes concernées dont les données personnelles sont transférées**

Les données personnelles transférées concernent les catégories de personnes concernées suivantes :

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

### **Catégories de données personnelles transférées**

- Le nom du client, le montant à payer, la date et l'heure, les détails du compte bancaire, les détails de la carte de paiement, le code CVC, le code postal, le code de pays, l'adresse, l'adresse de courriel, le télécopieur, le téléphone, le site Web, les données d'expiration, les détails d'expédition, le statut fiscal, l'identifiant unique du client, l'adresse IP, la localisation et toute autre donnée reçue par PayPal en vertu du Contrat.

### **Données sensibles (le cas échéant) et Restrictions ou mesures de protection appliquées**

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

- Non applicable, sauf si le marchand configure le service pour collecter ces données.

Applique des restrictions et des mesures de protection :

- Non applicable, sauf si le marchand configure le service pour collecter ces données.

### **Nature du traitement**

Tels qu'ils sont énoncés dans les conditions d'utilisation.

## **Objectif(s) du ou des transferts**

Le transfert est effectué aux fins suivantes :

- Performance des services fournis par l'importateur de données à l'exportateur de données conformément aux conditions d'utilisation.
- pour identifier les activités frauduleuses et les risques qui affectent ou pourraient affecter l'importateur de données, l'exportateur de données ou d'autres clients de l'importateur de données;
- pour se conformer aux lois applicables à l'importateur de données;
- Tel qu'indiqué dans l'Addenda sur la protection des données.

## **La période pendant laquelle les données personnelles seront conservées ou, si cela n'est pas possible, les critères utilisés pour déterminer cette période**

L'importateur de données ne conserve les données à caractère personnel que pendant la durée nécessaire à la réalisation des objectifs pour lesquels elles ont été collectées (voir les objectifs ci-dessus). Pour déterminer la période de conservation appropriée pour les données personnelles, l'importateur de données tient compte de la quantité, de la nature et du caractère sensible des données personnelles, du risque potentiel de préjudice résultant d'une utilisation ou d'une divulgation non autorisée des données personnelles, des objectifs pour lesquels les données personnelles sont traitées et de la possibilité d'atteindre ces objectifs par d'autres moyens, ainsi que des exigences légales, réglementaires, fiscales, comptables ou autres applicables.

## **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 personnelles avec des fournisseurs de services tiers qui exécutent des services et 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 fournis en vertu du contrat, comme la vérification du client, le traitement des transactions ou le soutien à la clientèle, ou fournir un service à l'importateur de données qui prend en charge les services fournis dans le cadre du contrat, comme stockage. Lorsqu'il détermine la durée du traitement effectué par les fournisseurs de services tiers, l'importateur de données applique les critères fournis ci-dessus dans la présente annexe 1.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.

## **B. Mesures techniques et organisationnelles, y compris les mesures techniques et organisationnelles pour 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 du secteur, 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 solide processus de gestion du changement de PayPal protège la disponibilité continue et la résilience des données et des systèmes tout au long de leur cycle de vie en s'assurant que les modifications sont planifiées, approuvées, exécutées et vérifiées de manière appropriée. Le processus de gestion de la continuité des activités de la Société fournit un cadre pour renforcer la résilience de l'organisation avec la capacité d'une réponse efficace qui protège les intérêts de ses principales parties prenantes.

### **3. Reprise après sinistre.**

Le solide programme de reprise après sinistre de PayPal dispose de processus pour récupérer les informations ou les systèmes technologiques en cas de perturbation importante, en se concentrant sur les systèmes informatiques qui soutiennent les processus commerciaux et les activités des clients essentiels. L'infrastructure technologique de PayPal est hébergée 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. Tester, évaluer et examiner régulièrement l'efficacité des mesures techniques et organisationnelles.**

PayPal planifie, exécute et rend compte régulièrement des résultats du programme de tests de la société afin d'évaluer et d'examiner 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 en utilisant un identifiant de compte et un mot de passe uniques pour l'identification et l'authentification de l'utilisateur avant d'accéder à toute autre application du champ d'application. Des politiques automatisées concernant la composition, la longueur, la modification, la réutilisation et le verrouillage des mots de passe sont appliquées. L'accès basé sur les rôles et les approbations, qui sont certifiés tous les trimestres, sont mis en œuvre dans tous les systèmes concernés afin d'appliquer le principe de moindre privilège.

**6. Sécurité physique des lieux où les données personnelles sont traitées.**

Les politiques et processus mondiaux de PayPal en matière de sûreté et de sécurité énoncent les exigences nécessaires pour faciliter les processus de sûreté et de sécurité solides, y compris la sécurité physique, conformément aux lois, règlements et exigences des partenaires applicables. L'accent 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 règles de sécurité de l'information de la Société.

**7. Enregistrement et configuration des événements.**

PayPal a décrit et défini les types et les attributs d'enregistrement et de surveillance des événements. L'entreprise collecte et regroupe plusieurs types d'enregistrement vers le système centralisé de surveillance de la sécurité. Un contrôle de gestion de la configuration standard est en place pour garantir que les enregistrements sont collectés à partir des systèmes, puis transmis à notre système centralisé de surveillance de la sécurité. Les politiques de PayPal et les processus

de soutien stipulent que la configuration du système et les lignes de base de durcissement doivent être mises en œuvre dans tous les systèmes.

**8. Gouvernance et gestion informatique; Certification et assurance des processus et des produits.**

PayPal promeut une philosophie de sécurité solide dans l'ensemble de l'entreprise. Notre responsable de la sécurité des informations supervise la sécurité des informations dans l'ensemble de notre entreprise. Dans le cadre de notre programme de gestion des risques et de la conformité de l'entreprise, notre programme de surveillance 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 et à identifier, protéger, détecter, répondre et se remettre des menaces à la sécurité de l'information. PayPal certifie et assure ses processus et ses produits par le biais de divers 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 cartes de paiement (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 précoce 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 recueillis et générés soient ceux qui sont adéquats, pertinents et limités à ce qui est nécessaire par rapport aux fins pour lesquelles 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 d'accès et de qualité de PayPal garantit que toutes les données personnelles sont correctes, complètes et à jour, permettant aux utilisateurs individuels d'accéder au système pour corriger et modifier leurs données personnelles (par exemple, leur adresse, leurs coordonnées, etc.) et, lorsqu'une demande de correction est reçue de la part d'une personne concernée, de fournir un service qui lui donne droit à la correction. Notre programme de gouvernance des

données surveille 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 informations sont éliminées, 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 de l'industrie et conçus pour susciter la collaboration et le partenariat des parties prenantes en matière de sensibilisation et de conformité à ces politiques et contrôles dans l'ensemble de l'organisation, afin de garantir la participation et la responsabilité partant de la haute direction vers le bas de l'organisation. Chaque programme définit les responsabilités pour les décisions, les processus et les contrôles pluridisciplinaires liés aux données. En tant que responsable du traitement de données, PayPal est responsable et démontre sa conformité aux articles pertinents portant une obligation de responsabilité dans le RGPD et d'autres lois de protection des données applicables par la mise en œuvre d'une politique de programme 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 de : 1) une solide culture de conformité, 2) 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) 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) un service mondial de 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) les communications avec l'entreprise par la fonction de confidentialité mondiale pour promouvoir la sensibilisation et la compréhension de la vie privée, 6) le 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 la vie privée, la gestion des problèmes liés à la vie privée, la formation à la vie privée, le plan annuel de protection de la vie privée, et 7)

les 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 pour s'assurer que les droits des personnes concernées sont respectés, y compris l'accès, la correction et l'effacement des données. Les demandes d'effacement de données sont traitées, sauf si PayPal a une obligation légale ou réglementaire ou un autre motif commercial 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 le biais d'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 embauchés.

## **B. Ce qui suit s'applique uniquement aux Clauses de transfert du Royaume-Uni**

### **Destinataires**

Les données personnelles transférées peuvent être divulguées uniquement aux destinataires suivants :

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

### **Informations d'enregistrement de la protection des données de l'exportateur de données (le cas échéant)**

Non applicable.

### **Informations complémentaires utiles (limites de stockage et autres informations pertinentes)**

Tels qu'ils sont énoncés dans les conditions d'utilisation.