>> **Ver todos los acuerdos legales**

Anexo de Protección de Datos de PayPal para productos de procesamiento de tarjetas

Última actualización: 10 de diciembre de 2021

Este Anexo de Protección de Datos de PayPal para Productos de Procesamiento de Tarjetas (este "Anexo") se aplica a cualquier producto, servicio u otra oferta en la que un miembro del Grupo PayPal ("PayPal") proporcione servicios de procesamiento de tarjetas, plataforma o protección contra fraudes (los "Servicios de Pago") a usted, al Comercio (el "Comercio" o "Usted"). Este Anexo no se aplica a los servicios de cartera de PayPal, como Pago con PayPal, ni a las ofertas de Pay Later de PayPal. Este Anexo formará parte del acuerdo pertinente entre el Comercio y PayPal que rige la prestación de Servicios de Pago por parte de PayPal a Usted (el "Acuerdo") y se incorpora por referencia en dicho acuerdo. En caso de que exista algún conflicto entre las condiciones de este Anexo y el Acuerdo, prevalecerán las condiciones de este Anexo. Los términos con mayúscula inicial utilizados en este Anexo, pero no definidos en él, tendrán el significado establecido en el Acuerdo.

Este Anexo entra en vigor a partir de (i) la fecha de entrada en vigor que se especifica en el Acuerdo, o bien (ii) la fecha de entrada en vigor mencionada en la notificación que se publique o se le envíe en relación con este Anexo. Es posible que modifiquemos periódicamente este Anexo. La versión modificada entrará en vigor en el momento en que la publiquemos en nuestro sitio web, a menos que se indique lo contrario. Si nuestros cambios reducen sus derechos o aumentan sus responsabilidades, publicaremos una notificación en la página "**Actualizaciones de las políticas**" de nuestro sitio web dentro del plazo exigido por el Acuerdo. Si no está de acuerdo con algún cambio en este Anexo, puede suspender el uso que hace de los Servicios de Pago.

Definiciones

Los términos que se indican a continuación tienen los siguientes significados cuando se utilizan en este Anexo:

"Controlador" significa una entidad que determina los fines y los medios del procesamiento de los Datos del Cliente. Sin embargo, si dicho término (o términos que se refieren a funciones similares) se define en las Leyes de Protección de Datos, "Controlador" tendrá el mismo significado que se le atribuya en la Ley de Protección de Datos aplicable.

"**Cliente**" se refiere a los clientes que utilizan los Servicios de Pago y, a los efectos de este Anexo, son interesados.

"**Datos del Cliente**" se refiere a los Datos Personales que: (i) el Cliente proporciona al Comercio y el Comercio transmite a PayPal mediante el uso de los Servicios de Pago, y (ii) PayPal puede recopilar del dispositivo y el navegador del Cliente mediante el uso por parte del Comercio de los Servicios de Pago.

"**Leyes de Protección de Datos**" se refiere a cualquier ley, reglamento, directiva, requisito normativo y código de prácticas de protección de datos aplicables a la prestación de Servicios de Pago, incluidas todas las modificaciones a dicha normativa y cualquier reglamento o instrumento asociado (por ejemplo, la Ley de Privacidad del Consumidor de California de 2018, Código Civil de California § 1798.100 et seq, el Reglamento General de Protección de Datos (UE) 2016/679 (RGPD), la Ley de Privacidad de Australia de 1988, la Ley de Protección de Información Personal y Documentos Electrónicos (Canadá), la Ordenanza de (Privacidad de) Datos Personales (cap.486) (Hong Kong), la Ley General de Protección de Datos de Brasil, la Ley Federal número 13709/2018 y la Ley de Protección de Datos Personales de 2012 de Singapur.

"Grupo PayPal" se refiere a PayPal, Inc. y a todas las empresas en las que PayPal o su sucesor posea o controle directa o indirectamente de vez en cuando.

"**Datos Personales**" se refiere a toda la información relacionada con una persona física identificada o identificable (un "interesado"). Una persona física identificable es aquella que se puede identificar, de forma directa o indirecta, en particular por medio de una referencia a un identificador tal como un nombre, un número de identificación, datos de ubicación, un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de dicha persona física.

"**Proceso**" o los términos que se refieran a funciones similares de protección de datos y privacidad cuando se utilicen en este Anexo tendrán el mismo significado que se les atribuye en las Leyes de Protección de Datos aplicables.

PayPal como Controlador

PayPal cumplirá con los requisitos de las Leyes de Protección de Datos aplicables a los Controladores en relación con el Procesamiento de Datos del Cliente en virtud de este Anexo (lo que incluye, entre otros, la implementación y el mantenimiento en todo momento de todas las medidas de seguridad correspondientes al Procesamiento de Datos del Cliente) y no hará ni permitirá deliberadamente que se haga algo con respecto a los Datos del Cliente que pueda llevar a un incumplimiento por parte del Comercio de las Leyes de Protección de Datos. PayPal solo transferirá los Datos del Cliente a terceros, subprocesadores o miembros del Grupo PayPal que firmen acuerdos por escrito que contengan términos para la protección de los Datos del Cliente, los cuales no deben proporcionar menos protección que los términos establecidos en este Anexo.

Procesamiento de Datos del Cliente en relación con los Servicios de Pago

Las partes reconocen y aceptan que el Comercio y PayPal son Controladores independientes en lo que respecta a todos los Datos del Cliente Procesados en relación con los Servicios de Pago. Por lo tanto, PayPal determina de manera independiente el propósito y los medios del Procesamiento de dichos Datos del Cliente, y no actúa como Controlador conjunto con el Comercio respecto de dichos Datos del Cliente.

Las partes reconocen y aceptan que PayPal tiene permitido utilizar, reproducir y procesar los Datos del Cliente y los datos de las transacciones de pago solo con los siguientes fines:

- según sea razonablemente necesario para proporcionar y mejorar los Servicios de Pago al Comercio y a sus Clientes, incluidas las herramientas de protección contra fraudes;
- monitorear, prevenir y detectar transacciones de pago fraudulentas, y prevenir daños al Comercio, a PayPal y a terceros;
- cumplir las obligaciones legales o normativas aplicables al Procesamiento y la retención de los datos de pago a las que está sujeto PayPal, incluidas las obligaciones aplicables de verificación de identidad y contra el lavado de dinero;
- analizar, desarrollar y mejorar los productos y servicios de PayPal;
- tener uso interno, lo que incluye, entre otros, análisis y métricas de datos;
- compilar y divulgar Datos del Cliente y datos de transacciones de pago en el agregado donde los Datos del Cliente individual o del usuario no se pueden identificar, lo que incluye un desglose de sus promedios por región o industria;

- cumplir los requisitos legales aplicables y colaborar con los organismos de seguridad proporcionando respuestas a las solicitudes de divulgación de información, de conformidad con las leyes, y
- cualquier otro fin para el cual notifique al Comercio, siempre y cuando dicho fin se ajuste a las Leyes de Protección de Datos.

Notificación a los Clientes por parte del Comercio

El Comercio (i) notificará a los Clientes en su Política de Privacidad que, a los fines del Procesamiento de los Datos del Cliente, PayPal es un Responsable del Tratamiento independiente, tal como se describe en este Anexo, y (ii) incluirá un enlace al Aviso de Privacidad de PayPal, disponible en **www.paypal.com**, en la política de privacidad del Comercio.

Asistencia mutua

Las partes aceptan cooperar entre sí en la medida en que sea razonablemente necesario para que la otra parte pueda desempeñar de forma adecuada su responsabilidad como Controladora independiente de conformidad con las Leyes de Protección de Datos. Las partes aceptan que, si el Comercio recibe del Cliente una solicitud de acceso a sus datos, o bien este ejerce cualquiera de sus derechos en virtud de las Leyes de Protección de Datos, el Comercio responderá directamente a la solicitud de acceso de dicho Cliente. El comercio también deberá informar al Cliente que puede ejercer los derechos de los interesados en relación con los Servicios de Pago con PayPal de acuerdo con las instrucciones descritas en el Aviso de Privacidad disponible en **www.paypal.com.** Asimismo, si en relación con algún incidente de seguridad, PayPal determina, de modo unilateral, que debe notificar a los Clientes afectados y no tiene la información de contacto necesaria de un Cliente afectado como para realizar dicha comunicación, el Comercio realizará todo esfuerzo que sea razonable desde el punto de vista comercial para proporcionar a PayPal la información del Cliente que pueda poseer con el único propósito de que PayPal pueda cumplir con las obligaciones de notificación aplicables en relación con los Clientes afectados, de conformidad con las Leyes de Protección de Datos.

Transferencias de datos transfronterizas

Las partes acuerdan que PayPal puede transferir los Datos del Cliente Procesados en virtud de este Acuerdo fuera del país donde se recopilaron según sea necesario para proporcionar los Servicios de Pago. Si PayPal transfiere los Datos del Cliente protegidos en virtud de este Anexo a una jurisdicción para la cual la autoridad reguladora aplicable para el país en que se recopilaron

los datos no ha emitido una decisión adecuada, PayPal se asegurará de que se hayan aplicado medidas de seguridad adecuadas para la transferencia de Datos del Cliente de conformidad con las Leyes de Protección de Datos aplicables. Por ejemplo, y para fines de cumplimiento del RGPD, nos basamos en normas corporativas vinculantes aprobadas por las autoridades de fiscalización competentes y otros mecanismos de transferencia de Datos del Cliente a otros miembros del Grupo PayPal.

En lo que respecta a las transferencias que Usted realice a PayPal de los datos de sus Clientes ubicados en la Unión Europea, Suiza, el Espacio Económico Europeo o sus Estados miembros, y el Reino Unido, acordamos que: (i) en la medida en que corresponda, se considerará que su firma del Acuerdo supone la firma y la aceptación de la Decisión de Ejecución (UE) 2021/914 de la Comisión Europea del 4 de junio de 2021 sobre las cláusulas contractuales estándar para la transferencia de datos personales a terceros países de conformidad con el RGPD ("Cláusulas de Transferencia de la UE") por parte del Comercio en cuanto exportador de datos y en su rol de responsable del tratamiento, y también supone la firma y la aceptación de las cláusulas estándar de protección de datos especificadas en los reglamentos dictados por el Secretario de Estado en virtud de la sección 17C (b) de la Ley de Protección de Datos de 2018 y, por el momento, en vigor en el Reino Unido (las "Cláusulas de Transferencia del Reino Unido") en cuanto exportador de datos; (ii) en la medida en que corresponda, se considerará que la firma del Acuerdo por parte de PayPal supone la firma y aceptación de las Cláusulas de Transferencia de la UE por parte de PayPal en cuanto importador de datos y en su rol de responsable del tratamiento, y también supone la firma y aceptación de las Cláusulas de Transferencia del Reino Unido en cuanto importador de datos; y (iii) las partes estarán sujetas a las disposiciones del Módulo 1 de las Cláusulas de Transferencia de la UE. En caso de que la Comisión Europea o el Secretario de Estado del Reino Unido (u otro organismo autorizado del Reino Unido aplicable) revise y luego publique nuevas Cláusulas de Transferencia de la UE o del Reino Unido, respectivamente —o según lo exija o implemente la Comisión Europea o el Secretario de Estado del Reino Unido (u otro organismo autorizado del Reino Unido aplicable)—, las partes acuerdan que dichas Cláusulas de Transferencia de la UE o el Reino Unido nuevas sustituirán, según corresponda, a las Cláusulas de Transferencia de la UE o del Reino Unido actuales, y aceptarán tomar todas las medidas necesarias para la ejecución de dichas cláusulas nuevas, según corresponda. Las Cláusulas de Transferencia de la UE (Módulo 1) y las Cláusulas de Transferencia del Reino Unido se incorporarán al Acuerdo por referencia y se considerarán debidamente ejecutadas entre las partes en la fecha de entrada en vigor del presente Acuerdo, con sujeción a los siguientes detalles:

A) Cláusulas de Transferencia de la UE

1. Se aplicará la opción 1 de la cláusula 17 (Derecho aplicable) y las leyes de Luxemburgo regirán las Cláusulas de la UE.
2. De conformidad con la cláusula 18 (Elección del foro y jurisdicción), los tribunales de Luxemburgo resolverán cualquier controversia que surja de las Cláusulas de la UE.
3. Las partes acuerdan que los detalles requeridos en el Apéndice de Cláusulas de Transferencia de la UE serán los establecidos en el Apéndice 1.

B) Cláusulas de transferencia del Reino Unido

1. Se incorpora la cláusula II(h)(iii), y la firma del Acuerdo por parte de PayPal se considerará la firma requerida de PayPal en cuanto importador de datos.
2. Las partes acuerdan que los detalles requeridos en el Anexo B de las Cláusulas de Transferencia del Reino Unido serán los establecidos en el Apéndice 1 (en la medida que corresponda).

Apéndice 1

Apéndice de la Cláusulas de Transferencia de la UE y Anexo B de las Cláusulas de Transferencia del Reino Unido

A. Lo siguiente se aplica, en la medida en que sea necesario, en virtud de las Cláusulas de Transferencia de la UE y las Cláusulas de Transferencia del Reino Unido

Anexo 1.A. Lista de partes

Exportador de datos

- Nombre y dirección: el exportador de datos es el Comercio, y la dirección es la estipulada en el Acuerdo.
- Nombre, cargo y detalles de contacto de la persona de contacto: según se estipula en el Acuerdo.
- Actividades pertinentes a los datos transferidos en virtud de la Cláusula Contractual Estándar: tal como se estipula en el Acuerdo.
- Firma y fecha: consulte la sección “Transferencias internacionales” de este Anexo.
- Función (responsable del tratamiento/procesador): responsable del tratamiento.

Importador de datos

- Nombre y dirección: el importador de datos es miembro del Grupo PayPal que presta los servicios de conformidad con el Acuerdo, y la dirección es la estipulada en el Acuerdo.
- Nombre, cargo y detalles de contacto de la persona de contacto: según se estipula en el Acuerdo.
- Actividades pertinentes a los datos transferidos en virtud de la Cláusula Contractual Estándar: tal como se estipula en la firma y la fecha del Acuerdo. Consulte la sección "Transferencias internacionales" de este Anexo.
- Función (responsable del tratamiento/procesador): responsable del tratamiento.

Anexo 1.B. Descripción de la transferencia

Sujetos de datos cuyos datos personales se transfieren

Los datos personales transferidos conciernen a las siguientes categorías de sujetos de datos:

- Los clientes, empleados y otros contactos de la empresa del exportador de datos.

Categorías de datos

Los Datos Personales transferidos pueden incluir las siguientes categorías de datos:

- nombre, importe por cobrar, fecha y hora, detalles de la cuenta bancaria, información de la tarjeta de pago, código CVC, código postal, código de país, dirección, dirección de correo electrónico, fax, teléfono, sitio web, datos de fecha de vencimiento, detalles de envío, situación fiscal, identificador único del cliente, dirección IP, ubicación y cualquier otro dato que PayPal haya recibido en virtud de este Acuerdo.

Datos confidenciales (si corresponde) y medidas de seguridad o restricciones aplicadas

Los datos personales transferidos conciernen a las siguientes categorías de datos confidenciales:

- No aplicable, a menos que el Comercio configure el servicio para capturar dichos datos.

Aplicación de restricciones y medidas de seguridad:

- No aplicable, a menos que el Comercio configure el servicio para capturar dichos datos.

Propósitos de las transferencias

La transferencia se realiza con los siguientes fines:

- Prestación de los servicios provistos por el importador de datos al exportador de datos de conformidad con el Acuerdo.

- Identificación de actividades fraudulentas y de los riesgos que afectan o pueden afectar al importador de datos, al exportador de datos o a otros clientes del importador de datos.
- Cumplimiento de las leyes aplicables al importador de datos.
- Fines establecidos en el Anexo de Protección de Datos.

Período durante el cual se retendrán los datos personales o, si no es posible, criterios utilizados para determinar ese período

El importador de datos solo retiene los datos personales durante el tiempo que sea necesario en relación con los fines pertinentes para los que se recopilaron (consulte los fines antes mencionados). Con el fin de determinar el período de retención adecuado para los datos personales, el importador de datos analiza el importe, la naturaleza y confidencialidad de los datos personales, el riesgo potencial de daño por uso o divulgación no autorizados de dichos datos, los fines para los que estos se procesan y si se pueden lograr dichos fines por otros medios, y los requisitos legales normativos, tributarios, contables o de otro tipo aplicables.

Para transferencias a (sub)procesadores, también especifique el asunto, la naturaleza y la duración del procesamiento

El importador de datos puede compartir datos personales con proveedores de servicios externos que prestan servicios y desempeñan funciones en la dirección del importador de datos y en nombre de este. Estos proveedores de servicios externos pueden, por ejemplo, proporcionar un elemento de los servicios prestados en virtud del Acuerdo, como la verificación de clientes, el procesamiento de transacciones o el servicio de atención al cliente; o prestar al importador de datos un servicio que respalda los servicios prestados en virtud del Acuerdo, como el almacenamiento. Al determinar la duración del procesamiento llevado a cabo por los proveedores de servicios externos, el importador de datos aplica los criterios proporcionados anteriormente en este Anexo 1.B.

Anexo 1.C. Autoridad supervisora

De conformidad con la cláusula 13(a) de las Cláusulas de Transferencia de la UE, la autoridad supervisora que tiene la responsabilidad de garantizar el cumplimiento del Reglamento (UE) 2016/679 por parte del exportador de datos en relación con la transferencia de datos, como se indicó, deberá actuar como autoridad supervisora competente.

B. Medidas técnicas y organizacionales, incluidas aquellas medidas técnicas y organizacionales destinadas a garantizar la seguridad de los datos

1. Seudonimización, cifrado y protección de los datos durante la transmisión

Las políticas de PayPal aseguran el cumplimiento de este principio y requieren el uso de controles técnicos para evitar el riesgo de divulgación de datos personales. PayPal utiliza cifrado en tránsito y en reposo para todos los datos personales. También utilizamos técnicas de seudonimización estándar del sector, como la tokenización para proteger los datos personales si corresponde. PayPal tiene políticas exhaustivas que proporcionan obligaciones y procesos clave para proteger los datos cuando se transfieren dentro de la empresa y externamente a terceros.

2. Administración de cambios y continuidad del negocio

El sólido proceso de administración de cambios de PayPal protege la disponibilidad continua y la resiliencia de los datos y sistemas a lo largo de su ciclo de vida para asegurar que los cambios se planeen, aprueben, ejecuten y revisen de forma adecuada. El proceso de administración de la continuidad del negocio de la Empresa proporciona un marco para establecer una resiliencia organizacional con capacidad de respuesta efectiva que proteja los intereses de las partes claves interesadas.

3. Recuperación ante desastres

El sólido programa de recuperación ante desastres de PayPal tiene procesos para recuperar la información o los sistemas tecnológicos en caso de cualquier interrupción significativa, con foco en los sistemas de TI que respaldan las actividades de clientes y los procesos comerciales de importancia crítica. La infraestructura tecnológica de PayPal se encuentra alojada en varios centros de datos seguros, con capacidad principal y secundaria, cada uno de ellos con infraestructura de red y seguridad, servidores dedicados de aplicaciones y bases de datos, y almacenamiento.

4. Prueba regular y evaluación de la efectividad de las medidas técnicas y organizacionales

PayPal planea, ejecuta e informa regularmente los resultados del programa de pruebas de la Empresa para evaluar la efectividad de sus medidas tecnológicas y organizacionales. La administración de este programa está a cargo de nuestro equipo de riesgo y cumplimiento

empresarial, el cual trabaja con las partes interesadas pertinentes para obtener y evaluar la información necesaria con fines de pruebas, informes y correcciones según sea necesario.

5. Identificación y autorización de usuarios

Los procesos de administración de acceso de PayPal requieren que los usuarios inicien sesión en la red corporativa utilizando una identificación y contraseña de cuenta únicas en esta red para identificar y autenticar al usuario antes de que pueda acceder a cualquier otra aplicación disponible. Se aplican políticas automatizadas en relación con la composición, longitud, cambio, reutilización y bloqueo de la contraseña. El acceso y las aprobaciones basadas en funciones, que se certifican trimestralmente, se implementan en todos los sistemas disponibles para hacer cumplir el principio del mínimo privilegio.

6. Seguridad física de las ubicaciones donde se procesan los datos personales

Las políticas y procesos de seguridad y protección globales de PayPal establecen los requisitos necesarios para facilitar procesos sólidos de seguridad y protección, incluida la seguridad física, de acuerdo con las leyes, reglamentos y requisitos aplicables de los socios. Se hace especial hincapié en los sistemas y medidas de seguridad al construir áreas especiales o críticas, como oficinas de correo, almacenamiento de equipos, áreas de envío y recepción, salas de computación o de servidores, almacenes de comunicaciones o áreas de almacenamiento de documentos e información clasificados en cumplimiento del estándar de manejo de seguridad de la información de la Empresa.

7. Registro y configuración de eventos

PayPal ha detallado y definido los tipos y atributos del registro y monitoreo de eventos. La Empresa recopila y agrega varios tipos de registros al sistema de monitoreo de seguridad centralizado. Existe un control de administración de configuración estándar para garantizar que los registros se recopilen de los sistemas y luego se reenvíen a nuestro sistema de monitoreo de seguridad central. Las políticas y los procesos de soporte de PayPal establecen que debe implementarse una línea base de configuración y protección del sistema en todos los sistemas.

8. Gestión y administración de TI, certificación y aseguramiento de procesos y productos

PayPal promueve una fuerte filosofía de seguridad en toda la Empresa. Nuestro director de seguridad de la información supervisa la seguridad de la información en toda nuestra empresa global. Como parte de nuestro Programa de Administración de Riesgos y Cumplimiento

Empresarial, nuestro Programa de Supervisión Tecnológica y Seguridad de la Información está diseñado para respaldar a la Empresa en la administración de riesgos de seguridad de la información y la tecnología, así como en cuestiones de identificación, protección detección, respuesta y recuperación en relación con las amenazas a la seguridad de la información. PayPal certifica y asegura sus procesos y productos mediante una variedad de programas empresariales, que incluyen (i) auditorías y evaluaciones de las obligaciones técnicas estándar del sector que PayPal debe cumplir, incluidas, entre otras: ISO 27001, los estándares aplicables de la industria de las tarjetas de pago (PCI) (como DSS, NIP, P2PE, etc.) y SOC-1 y SOC-2 del Instituto Estadounidense de Contadores Públicos Certificados (AICPA); (ii) un proceso de identificación del control de riesgos (RCIP) que garantiza acciones tempranas y un enfoque estándar respecto de la medición, la administración y el monitoreo del riesgo asociado con el desarrollo y el lanzamiento de soluciones de productos; (iii) evaluaciones de impacto en la privacidad que se integran en las primeras etapas de los procesos de desarrollo de productos y software; y (iv) un programa integral de administración de terceros, que proporciona garantías mediante la administración continua de riesgos a lo largo del ciclo de vida de interacción con un tercero.

9. Minimización de datos

Nuestras políticas requieren (mediante controles técnicos) que los elementos de datos recopilados y generados sean aquellos que son adecuados, pertinentes y limitados a lo que es necesario en relación con los fines para los que se procesan. Los procesos de evaluación de impacto en la privacidad de PayPal aseguran el cumplimiento de estas políticas.

10. Calidad y retención de datos

La política de acceso y calidad de PayPal garantiza que todos los datos personales sean correctos y estén completos y actualizados, lo que permite a los usuarios individuales acceder al sistema para corregir y modificar sus datos particulares (p. ej.: dirección, datos de contacto, etc.), y, cuando se recibe una solicitud de corrección de un interesado, garantiza la prestación de un servicio que permita ejercer su derecho a la corrección. Nuestro programa de gobernanza de datos monitorea la calidad, los problemas y las medidas correctivas en relación con los datos según sea necesario. Necesitamos que todos los datos se clasifiquen, de acuerdo con su valor para el negocio, con los períodos de retención asignados, lo cual se basa en los requisitos legales, normativos y de conservación de registros empresariales de PayPal. Tras el vencimiento del período de retención, los datos y la información se desecharán, borrarán o destruirán.

11. Responsabilidad

PayPal ha desarrollado un conjunto de políticas y principios de seguridad informática, tecnología, administración de datos, administración de terceros y privacidad que cumplen con los estándares de la industria y se diseñaron con el fin de asegurar la colaboración y asociación de las partes interesadas de una manera que tenga en cuenta dichos controles y políticas, y cumpla con ellos, en toda la organización para garantizar la participación y responsabilidad desde el nivel jerárquico hasta todos los niveles de la organización. Cada programa define responsabilidades para las decisiones, procesos y controles relacionados con datos interfuncionales. Como responsable del tratamiento de datos, PayPal es responsable de los artículos pertinentes que suponen una obligación de responsabilidad en el RGPD y otras leyes de protección de datos aplicables, y demuestra el cumplimiento de ellos, mediante la implementación de una política de programa de privacidad y una estructura de control técnico y organizacional subyacente por niveles para garantizar el cumplimiento de las leyes, reglamentos, políticas y procedimientos de privacidad en toda la empresa. Esto incluye poder demostrar el cumplimiento de las leyes de protección de datos mediante: 1) una fuerte cultura de cumplimiento; 2) una estructura de gestión de riesgo y cumplimiento empresarial que incluya comités de administración, cargos de supervisión y reportes de privacidad; 3) responsabilidad de la función de la empresa para el cumplimiento del programa de privacidad, que incluye establecimiento, documentación y mantenimiento de procesos y controles de la empresa; 4) un departamento de privacidad global dentro de la organización de cumplimiento empresarial, con el fin de supervisar el cumplimiento de la empresa con el programa de privacidad y definir políticas, estándares, procedimientos y herramientas puestos en marcha por las funciones de la empresa; 5) comunicaciones para la empresa (por la función de privacidad global) a fin de promover la comprensión y comprensión de la privacidad; 6) Marco de administración de riesgos y cumplimiento empresarial para garantizar el uso de procesos coherentes, incluidas evaluaciones de impacto, monitoreo, pruebas, administración de problemas y capacitación en privacidad, plan de privacidad anual y 7) reportes y análisis a los comités de administración que supervisan el Programa de privacidad.

12. Derechos del interesado

PayPal tiene un programa implementado para garantizar que se cumplan los derechos de los interesados, incluidos los relacionados con el acceso, la corrección y el borrado. Se cumplirán las solicitudes de borrado de datos, a menos que PayPal tenga una obligación legal o reglamentaria, u otra razón empresarial legítima para retenerlos. Las políticas de PayPal garantizan que el borrado se produzca a lo largo del ciclo de vida del cliente.

13. Procesadores

PayPal tiene un programa de administración externo exhaustivo que proporciona garantías por medio de la administración continua de riesgos a lo largo del ciclo de vida de una interacción con un tercero. Contamos con controles contractuales para requerir que nuestros procesadores y los subprocesadores de estos proporcionen estándares exhaustivos de seguridad y privacidad de datos en toda la cadena de procesamiento. Todos los subprocesadores deben solicitar nuestra aprobación antes de su incorporación.

La siguiente información se aplica únicamente a las Cláusulas de Transferencia del Reino Unido

Destinatarios

Los datos personales transferidos pueden divulgarse solo a los siguientes destinatarios:

- los proveedores de servicios de los importadores de datos (como se detalla más arriba), sus filiales y el personal que presta los servicios de conformidad con el Acuerdo.

Información de registro de protección de datos del exportador de datos (si corresponde)

No aplicable.

Información adicional útil (límites de almacenamiento y otra información relevante)

Tal como se establece en el Acuerdo.