PayPal

>> Ver todos los acuerdos legales

Cláusulas Contractuales Tipo de Responsable a Responsable

 Imprimir  Descargar PDF

Última actualización: 8 de junio de 2022

Estas Cláusulas Contractuales Tipo de Responsable a Responsable ("SCC") forman parte de las Condiciones de Uso de PayPal aplicables (el "Acuerdo") entre usted, como vendedor ("usted" o el "Comercio"), y PayPal, y se incorporan por referencia en dicho acuerdo. En caso de que exista algún conflicto entre las condiciones de estas SCC y el Acuerdo, prevalecerán las condiciones de estas SCC. Los términos con mayúscula inicial utilizados en estas SCC, pero no definidos en ellas, tendrán el significado establecido en el Acuerdo.

En la medida en que sea aplicable: (i) se considerará que su firma del Acuerdo supone la firma y aceptación de la Decisión de Ejecución (UE) 2021/914 del 4 de junio de 2021 de la Comisión Europea relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 ("Cláusulas de Transferencia de la UE") por parte del Comercio en cuanto exportador de datos y en su rol de responsable del tratamiento; (ii) 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 (iii) que 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 revise y luego publique nuevas Cláusulas de Transferencia de la UE (o, de algún otro modo, las requiera o implemente), las partes acuerdan que esas nuevas Cláusulas de Transferencia de la UE reemplazarán a las actuales y que tomarán todas las medidas necesarias para la ejecución de las nuevas Cláusulas de Transferencia de la UE.

Las Cláusulas de Transferencia de la UE (Módulo 1) se incorporarán al Acuerdo por referencia y se considerarán debidamente ejecutadas entre las partes en la fecha de entrada en vigor del Acuerdo con sujeción a los siguientes detalles:

i. Se aplicará la opción 1 de la cláusula 17 (Derecho aplicable), y las leyes de Luxemburgo regirán las Cláusulas de Transferencia la UE.

i. De conformidad con la cláusula 18 (Elección del foro y jurisdicción), los tribunales de Luxemburgo resolverán cualquier controversia que surja de las Cláusulas de Transferencia la UE.

ii. Las partes acuerdan que los detalles requeridos en el Apéndice de Cláusulas de Transferencia de la UE serán los establecidos en el Apéndice 1.

Apéndice 1

Apéndice de Cláusulas de Transferencia de la UE

Anexo 1.A. Lo siguiente se aplica, en la medida en que sea necesario, en virtud de las Cláusulas de Transferencia de la UE

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 lo establecido en estas SCC
- 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 el Acuerdo.
- Firma y fecha: consulte lo establecido en estas SCC
- Función (responsable del tratamiento/procesador): responsable del tratamiento.

Anexo 1.B. Descripción de la transferencia

Interesados cuyos datos personales se transfieren
Los datos personales transferidos conciernen a las siguientes categorías de interesados:

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

Categorías de datos personales transferidos

- 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.

Naturaleza del procesamiento

Tal como se establece en el Acuerdo.

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.
- Para cumplir con las leyes y las solicitudes de cumplimiento de la ley aplicables al importador de datos.
- Con los fines establecidos en el Aviso de privacidad del importador 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 en estas SCC, 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 los 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. Gobernanza 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 a los datos y su corrección y 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 implementen 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.