Acerca de

Con la presente Política de Privacidad, nos gustaría informarle sobre la naturaleza, el alcance y la finalidad de la recogida y el tratamiento de sus datos personales cuando utilice nuestra app móvil o nuestro sitio web, www.vivid.money, operados por Vivid Money GmbH («Vivid Money», «nosotros», «nos»).

Autoridad responsable

El responsable de la recogida y el tratamiento de sus datos personales de acuerdo con el Reglamento General de Protección de Datos de la UE (Reglamento (UE) 2016/679) («RGPD») es:

Vivid Money GmbH
Kemperplatz 1
10785 Berlín, Alemania
N.º de inscripción en el Registro Mercantil alemán (HRB): 209049 B

Si usted tiene alguna inquietud, solicitud o pregunta sobre sus datos, o piensa que algunas de nuestras prácticas de privacidad no están contempladas en esta Política de Privacidad, póngase en contacto con nuestro delegado de protección de datos a través de la dirección de correo electrónico dpo@vivid.money.

Corresponsables del tratamiento

Asimismo, tenga en cuenta que, para poder ofrecerle a usted nuestros productos bancarios, trabajamos en estrecha colaboración con Solaris SE («Solaris»), cuya dirección es Cuvrystraße 53, 10997, Berlín, Alemania. Solaris puede que opere a través de una sucursal local en el país en el que usted resida. Dada su naturaleza de organismo con licencia bancaria, Solaris dispone de la infraestructura necesaria para prestar servicios bancarios, y Vivid Money actúa como su plataforma tecnológica. Operamos la app bancaria, prestamos el servicio al cliente y, junto con Solaris, gestionamos los depósitos de los clientes. Nosotros y Solaris determinamos conjuntamente los fines y medios del tratamiento de sus datos personales sobre la base de un acuerdo de corresponsabilidad según el significado que le otorga el artículo 26 del RGPD.

En esencia, usted concluye un acuerdo marco de servicios de pago con Solaris, así como un contrato de uso con nosotros. A fin de concluir y ejecutar los respectivos contratos y de prestar nuestros servicios, nosotros y Solaris debemos recoger sus datos personales. Nosotros y el banco actuamos como corresponsables de estos datos, lo que significa que, en general, cualquier recogida, tratamiento y uso de datos personales con respecto a la prestación de servicios bancarios es responsabilidad del banco, mientras que por lo que respecta al contrato de uso la responsabilidad recae sobre nosotros.

Entre otras cosas, el acuerdo de corresponsabilidad del tratamiento especifica que usted puede hacer valer todos los derechos relacionados con el tratamiento de sus datos contra nosotros y Solaris.

Si desea recibir información más detallada sobre nuestras obligaciones y las del Solaris, póngase en contacto con nosotros a través de la dirección de correo electrónico privacy@vivid.money.

Si usted desea más información sobre cómo Solaris trata sus datos personales, podrá encontrarla en https://vivid.money/en-de/legal-documents/. Dicha información estará en su idioma y vendrá específicamente referida al país en el que usted resida.

Por qué tratamos sus datos personales (base jurídica)

1. Contrato

Al descargar nuestra app, usted tiene la oportunidad de abrir una cuenta corriente en nuestro banco asociado Solaris. Se necesitan determinados datos personales para suscribir este acuerdo y para la posterior prestación de los servicios incluidos. El tratamiento de los datos lo llevamos a cabo nosotros, Solaris y cualquier otro tercero que nos ayude a prestarle servicios financieros. La base jurídica de dicho tratamiento es el artículo 6, apartado 1, letra *b*) del RGPD: el tratamiento es necesario para la ejecución de un contrato en el que usted es parte o para la aplicación a petición de usted de medidas precontractuales.

Tenga en cuenta que para muchos de nuestros servicios financieros y funciones, sin los datos personales necesarios no podremos cumplir nuestras obligaciones contractuales, y, por consiguiente, es probable que debamos negarnos a entablar una relación comercial con usted, o bien nos veamos obligados a terminarla.

2. Intereses legítimos

En ocasiones necesitamos recoger y tratar sus datos personales para salvaguardar nuestros intereses legítimos o los intereses legítimos de terceros. En estos casos, también tratamos sus datos de forma lícita de acuerdo con el artículo 6, apartado 1, letra *f*) del RGPD. Ejemplos de dicho tratamiento son, entre otros, los siguientes:

- Garantía de la seguridad informática
- Prevención de actividades delictivas, como el fraude (para este fin recopilamos datos sobre su dispositivo y sobre su sesión)
- Envío de notificaciones push o mensajes relacionados con sus servicios y ofertas existentes o nuevos
- Análisis y optimización de la experiencia del usuario
- Personalización de servicios y opciones de tarifas

- Defensa de reclamaciones y contra estas

3. Consentimiento

Si nos ha dado su consentimiento para tratar sus datos personales para uno o más de los siguientes fines específicos:

- Permitirnos mostrar a otros clientes que usted usa el banco con el que estamos asociados
- Añadir un avatar con foto y permitirnos mostrárselo a otros clientes, por ejemplo en las listas de contactos de estos, actividades bancarias compartidas o enlaces de referencia (si ha elegido ser visible como cliente)
- Acceder a los contactos de su dispositivo
- Colocar cookies en su dispositivo

Estos datos se tratan de acuerdo con el artículo 6, apartado 1, letra *a*) del RGPD. Puede retirar su consentimiento en cualquier momento; por ejemplo, eliminando la foto o accediendo a la configuración de la app o de su dispositivo para deseleccionar estas funciones. Sin embargo, debe tener en cuenta que el tratamiento que haya tenido lugar antes de la retirada de su consentimiento sigue siendo lícito.

Prevención del fraude y del blanqueo de capitales, SEON

Cuando se registre a través de nuestro aplicación del socio para utilizar los servicios bancarios prestados por Solaris SE, Cuvrystraße 53, 10997 Berlín, Alemania o su sucursal española, Solaris SE, Sucursal en España, y de forma continuada mientras utilice dichos servicios, Solaris realizará una evaluación de riesgos con fines de prevención del fraude y lucha contra el blanqueo de capitales. Para ello, Solaris recurre a SEON Technologies Kft. (Rákóczi út 42. 7. em., Budapest 1072, Hungría) como proveedor de servicios en virtud de un acuerdo de procesamiento de datos con Solaris de conformidad con el Art. 28 GDPR.

Para realizar la evaluación de riesgos, recopilamos y transferimos a Solaris los siguientes datos del navegador, datos del dispositivo, datos de tráfico y datos de ubicación de su dispositivo: Dirección IP, incluido el tipo (por ejemplo comercial, línea móvil, universidad) y si está catalogada como dañina, valor de TOR, VPN, proxy, número de accesorios conectados a su dispositivo, si su teléfono está silenciado o no, volumen del sistema del dispositivo, código de país y nombre del operador (a) asociado a la tarjeta SIM y (b) que el dispositivo está utilizando actualmente, el tipo de modelo del dispositivo y su identificador único, el tiempo de actividad del sistema, el token de iCloud, la versión y el nombre del dispositivo facilitados por el usuario en los ajustes de iOS, cuándo se inició el dispositivo por última vez en formato de hora UNIX y

zona horaria UTC, el código de país y el ID asociados al dispositivo, el ID de sesión de la cookie y los detalles/ajustes del navegador, incluido el comportamiento de desplazamiento.

Solaris puede añadir información adicional y, a continuación, transferirá dichos datos a SEON junto con su dirección de correo electrónico, nombre y número de teléfono para la realización de un análisis de riesgos en relación con posibles actividades fraudulentas u otras actividades ilícitas.

SEON analiza estos datos personales basándose en un procedimiento matemático-estadístico reconocido y probado y proporcionará a Solaris una puntuación de riesgo de fraude. Como parte del análisis, SEON puede realizar un análisis del correo electrónico, una búsqueda en las redes sociales o un perfil de direcciones.

información adicional

La tecnología Seon permite identificar y evaluar el riesgo de actividades fraudulentas e ilícitas. En concreto se pueden tratar la siguiente tipología de datos personales:

Dirección IP (incluido el tipo, como comercial / organización / biblioteca / línea fija / línea móvil / escuela, colegio, universidad / centro de datos, alojamiento web / reservado / militar / red de entrega de contenidos / gobierno / araña de motor de búsqueda), dirección de correo electrónico (incluido si existe), valor de puntuación relativo a la dirección de correo electrónico, booleano registrado o desechable, código de país IP, estado IP, latitud geográfica, longitud geográfica, valor TOR, si una dirección IP figura como dañina o no, VPN, proxy web, proxy público, número de listas de spam en las que se ha encontrado la dirección IP, historial de solicitudes de recalificación de la dirección IP basado en evaluaciones anteriores en SEON, detalles de la cuenta de redes sociales (si una cuenta está registrada en redes (de redes sociales) con la cuenta de correo electrónico, p. ej. g. Facebook, Google, Apple, Twitter, Microsoft, eBay, Yahoo, Instagram), detalles de las violaciones de datos si el correo electrónico se ha visto comprometido, historial de solicitudes relativas a la dirección de correo electrónico (basado en evaluaciones anteriores en SEON), número de teléfono, número de accesorios conectados al dispositivo, si el teléfono está silenciado o no, volumen del sistema del dispositivo en una escala de 0 a 100, si el teléfono se está cargando actualmente, nivel actual de la batería del dispositivo en una escala de 0 a 100. El código de país asociado a la tarjeta SIM, el número de teléfono del dispositivo, el número de teléfono del dispositivo, el número de teléfono del dispositivo y el número de teléfono del dispositivo, el código de país asociado a la tarjeta SIM, el nombre del operador asociado a la tarjeta SIM, el identificador único del dispositivo del usuario basado en el algoritmo de SEON, el tipo de modelo del dispositivo, el identificador único del dispositivo, el token de ubicuidad de iCloud registrado en el dispositivo, la versión y el nombre del dispositivo proporcionados por el usuario en los ajustes de iOS, la última vez que se inició el

dispositivo en formato de hora UNIX y zona horaria UTC, la red que utiliza actualmente el dispositivo y el código de país asociado al dispositivo.

SEON puede recopilar información adicional sobre las cuentas (de redes sociales) del usuario, como la URL del avatar, el nombre o la fecha de registro. Si está disponible públicamente, también podría incluir el análisis del dominio, la existencia de la cuenta, el sexo, la edad (según el perfil), la configuración del idioma, el estado de la relación, el lugar de trabajo y la evaluación de la actividad del perfil.

Para la huella digital del dispositivo: hash de cookies (ID de la sesión de cookies del navegador), hash del navegador (ID del entorno del navegador utilizando todos los datos recopilados del navegador / sistema operativo / dispositivo y red), hash del dispositivo (ID del entorno de hardware del dispositivo a través de la huella digital basada en canvas y html5):

- Parámetros recopilados de los navegadores: hash de cookies, hash del navegador, hash / identificador único del dispositivo, zona horaria del navegador e IP, detección del sistema operativo, información del agente de usuario, detección de navegación privada, idiomas del sistema operativo / navegador, tamaño de pantalla del dispositivo / navegador / ventanas, fuentes instaladas y hash generado, plugins instalados y hash generado, nivel de batería, información de GPU, cursor, comportamiento de desplazamiento, características del navegador: flash / java, etc., huella digital del dispositivo canvas, huella digital de audio, IPs WebRTC, DNS: Geo + ISP, huella digital TCP/IP, análisis pasivo de hand-shake SSL/TLS

- Parámetros recopilados de dispositivos IOS: hash / identificador único de dispositivo, información de accesorios, información de audio, información de batería, información de CPU, identificador de publicidad (ADID), nombre de dispositivo, orientación de dispositivo, identificador único de dispositivo (UDID), token de ubicuidad de iCloud, datos de versión de iOS, estado de jailbreak, detección de emulador, información del kernel, información de arranque, configuración de red, datos de la placa de circuito impreso, información de la memoria, datos del sensor de proximidad, idioma local, zona horaria local, brillo de la pantalla, resolución de la pantalla, tiempo de actividad del sistema, información de almacenamiento, dirección MAC, SSID WIFI, huella digital TCP/IP, análisis pasivo del protocolo SSL/TSL.

- Parámetros recopilados de dispositivos Android: hash/identificador único del dispositivo, ID de Android, datos de la versión de Android, información de au-dio, información de la batería, información de compilación, información del operador, información de la CPU, nombre del dispositivo, información de almacenamiento, detección del emulador, estado de root, información del kernel, información de arranque,

configuración de red, datos de la placa de circuito impreso, información de la memoria, datos del sensor de proximidad, idioma local, zona horaria local, brillo de la pantalla, resolución de la pantalla, tiempo de actividad del sistema, dirección MAC, SSID WIFI, huella digital TCP/IP, análisis pasivo del protocolo SSL/TSL.

En función del análisis y de la puntuación de riesgo, podrá completar su registro, ser rechazado como nuevo cliente o se le podrá guiar a través de un proceso de registro ampliado. El proceso de toma de decisiones está automatizado. Si desea impugnar la decisión automatizada y desea que un ser humano revise esta decisión automatizada, puede ponerse en contacto con nosotros dirigiéndose a [add email address]. Una vez que haya dado su consentimiento y esté incorporado, Solaris recopilará continuamente los datos anteriores y realizará análisis de riesgo adicionales a través de SEON para la evaluación continua del riesgo de fraude.

La base jurídica del tratamiento es su consentimiento (art. 25 TTDSG - si procede - , art. 6 (1) lit. a, Art. 22 (2) lit. a GDPR y otras disposiciones pertinentes sobre protección de datos aplicables en su jurisdicción).

Si bien usted es libre de dar su consentimiento, la comprobación de la prevención del fraude y de la lucha contra el blanqueo de capitales es necesaria para una prestación segura de los servicios bancarios por parte de Solaris. Como banco autorizado, Solaris tiene la obligación legal de luchar contra el blanqueo de capitales mediante el establecimiento de un sistema operativo de gestión de riesgos y medidas de seguridad internas, así como un control continuo de las actividades de los clientes (artículos 4, 6 y 10 de la Ley alemana contra el blanqueo de capitales y otras disposiciones pertinentes contra el blanqueo de capitales aplicables en su jurisdicción). Puede retirar su consentimiento en cualquier momento enviando un correo electrónico a privacy@vivid.money, pero sin su consentimiento no podrá seguir utilizando los servicios de Solaris. Como consecuencia de ello, tendremos que poner fin a nuestra relación con usted y también podrán verse afectados otros servicios disponibles a través de la aplicación móvil Vivid Money.

Sus datos personales se almacenarán hasta que se cumplan los fines del tratamiento de estos datos establecidos anteriormente, y se eliminarán en un plazo máximo de 12 meses tras la realización de la evaluación de riesgos, a menos que se apliquen obligaciones legales de conservación (por ejemplo, en virtud de la legislación en materia de prevención de blanqueo de capitales, mercantil o fiscal).

4. Obligación legal

En los casos en los que nosotros o nuestros socios estamos obligados a cumplir con cualquier legislación aplicable, sus datos personales se tratan de acuerdo con el artículo 6, apartado 1, letra *c*) del RGPD: el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

Algunos ejemplos de ese tratamiento son, entre otros, la verificación de su identidad y edad, la prevención del blanqueo de dinero y el fraude, y las obligaciones de declaración de impuestos.

Cuándo tratamos sus datos personales

Apertura de cuenta.
Para que usted pueda celebrar válidamente un contrato con Solaris cuyo objeto sea la apertura de una cuenta en su nombre, nosotros debemos, entre otros, recopilar los siguientes datos personales cuya titularidad usted ostenta: su dirección de correo electrónico, número de teléfono, nacionalidad, país de residencia, nombre completo, fecha de nacimiento, sexo, si tiene usted la condición de residente fiscal en EE. UU., su estado laboral, su dirección, su ID válido de cliente de Vivid Money (asignado por nosotros) y sus credenciales de inicio de sesión.

Verificación de identidad
Para poder abrirle una cuenta en Solaris, debe verificar su identidad. A tal efecto, le pedimos que se someta a un procedimiento de identificación por vídeo a través de un proveedor de servicios de terceros. Es posible que también deba presentar una copia de su documento de identidad oficial. Usted deberá proporcionar una copia de su documento de identidad expedido por su Gobierno.

Emisión y entrega de la tarjeta
Una vez que haya abierto la cuenta bancaria, puede pedir una tarjeta. Para hacerle una y entregársela, tratamos y transferimos a Solaris y a nuestros proveedores de servicios su nombre, dirección, número de teléfono, correo electrónico, identificador de dispositivo e información sobre la cuenta bancaria a la que está vinculada la tarjeta. Si se trata de una tarjeta virtual, tratamos todos los datos antes mencionados, salvo su dirección.

Transferencias y pagos
Cuando usted comienza a utilizar su cuenta y sus tarjetas bancarias, además de algunos de los datos personales proporcionados para la apertura de su cuenta tratamos los siguientes:

- Transferencias realizadas a su cuenta y desde esta (p. ej., números de cuenta internos y externos, IBAN (para transferencias externas), nombre o número de teléfono del destinatario, importe, divisa, fecha e identificador de cliente)
- Transacciones con tarjeta (p. ej., comercio, importe, divisa, ubicación, fecha, forma de pago e identificador de cliente)

Tenga en cuenta que cuando realice una transferencia de fondos a otra persona utilizando el número de teléfono de esta, debemos mostrar en su estado de cuenta mensual o anual, o cualquier otro documento bancario que refleje las transferencias realizadas a su cuenta y desde esta, el nombre y el número de cuenta del destinatario.

Solicitudes de dinero
Si envía una solicitud de dinero a otra persona o comparte gastos con sus amigos o familiares (hasta 10 personas, y solo a aquellas que hayan permitido ser visibles como clientes nuestros), mostraremos su nombre al destinatario. Su nombre y número de cuenta también aparecerán en el estado de cuenta mensual o anual de este, o en cualquier otro documento bancario que refleje las transferencias ejecutadas a la cuenta de este y desde dicha cuenta.

Compartir pocket
El propietario del pocket puede compartirlo con un máximo de cinco personas. Los nombres de esas cinco personas (nombre procedente del libro de clientes o nombre del cliente) y los detalles de todas las transacciones que estas ejecutan (p. ej., fecha, comercio, ubicación e importe) son visibles para el propietario del pocket y los demás usuarios de este. Los usuarios pueden verse entre sí y ver los detalles del pocket compartido, únicamente si lo aceptan. También pueden ver los detalles del propietario y las transacciones realizadas entre sí, así como los fondos disponibles en la cuenta. Ni el propietario ni los usuarios pueden ver los detalles de la tarjeta del otro.

Google Pay y Apple Pay
Añadir la tarjeta a Google Pay o Apple Pay implica el tratamiento de la información de dicha tarjeta y del identificador de Google Wallet o de Apple Wallet por nuestra parte y la de nuestro banco asociado. La información de su tarjeta se transfiere al proveedor de servicios de nuestro socio, Visa, donde se acorta (básicamente, se cifra). Posteriormente, la pasamos a Google o Apple junto con su dirección, número de teléfono y los últimos cuatro dígitos del número de la tarjeta. Estos utilizarán los datos cifrados de la tarjeta para realizar transacciones cuando usted pague con su teléfono móvil.

Información sobre pagos realizados utilizando Open banking (banca abierta)
Cuando usted utiliza banca abierta, sus datos personales son transmitidos a un tercero autorizado prestador de servicios de pagos. Tales datos incluirán su ID de cliente de Vivid Money, su dirección (cuando sea procedente), su IBAN y el nombre del banco al que está enviando su solicitud. Su nombre de usuario o identificador de inicio de sesión y su contraseña, cuya facilitación le será pedida, no son datos que nosotros recopilemos o almacenemos.

Visibilidad y acceso a la agenda de contactos del teléfono
Cuando te unes a Vivid, o más tarde, cuando utilizas por primera vez determinadas funciones de Vivid y actividades bancarias conjuntas como son los pockets compartidos, los enlaces de recomendación, las transferencias de dinero instantáneas o las solicitudes de dinero mediante número de teléfono, te pedimos tu consentimiento para que figures visible como usuario de Vivid ante otros clientes o para acceder a la agenda de contactos de tu teléfono a través de su sistema operativo.

Si nos das este permiso, aparecerá un icono de Vivid junto a tu foto en las listas de contactos de otros clientes dentro de la app Vivid, así como en las actividades bancarias conjuntas y los

enlaces de recomendación cuando interactúes con otros clientes de Vivid. Esto significa que otros clientes de Vivid que tengan tu número de teléfono en sus agendas de contactos podrán identificarte como usuario de Vivid. Puedes retirar este consentimiento en cualquier momento en la configuración del perfil de la app. El segundo consentimiento, que autoriza a Vivid a acceder a la agenda telefónica de tu dispositivo mediante el sistema operativo del teléfono, también puedes revocarlo directamente en la configuración de tu dispositivo.

Programa de cashback / puntos Vivid

En el contexto de nuestro programa de cashback/puntos, tratamos su identificador de cliente, así como los datos sobre sus transacciones, incluidos los detalles recibidos de los procesadores de pago acerca del importe, la fecha, la hora y el comercio. Asimismo, con el fin de verificar sus transacciones y calcular correctamente los importes de cashback, debemos compartir con los comercios o con nuestros socios de cashback algunos datos seudonimizados sobre sus transacciones: fecha/hora, importe de la operación y moneda, datos del comercio (código de categoría del comercio, identificador del comercio y nombre del comercio en caso de tratarse de operaciones con tarjeta, e IBAN y nombre del beneficiario en caso de domiciliación), país y ciudad de compra, identificador del adquirente e identificador del terminal. Si no desea que tratemos sus datos o los compartamos con este fin, puede oponerse a ello en cualquier momento, solo tiene que ponerse en contacto con nosotros por correo electrónico a la dirección privacy@vivid.money. Tenga en cuenta que no vendemos sus datos personales ni los compartimos con terceros para fines de marketing.

Protección de suscripción

Para ayudarle a equilibrar sus gastos y controlar su presupuesto, realizamos un seguimiento de todos los pagos regulares que se cargan a su cuenta y le notificamos cuando se va a realizar uno. De esa manera usted puede tomar medidas de antemano, en caso de que haya fondos limitados en su cuenta y el pago deba modificarse o cancelarse. En este proceso podemos tratar datos personales como su identificador de cliente, transacción de cuenta bancaria, y detalles del comercio, fecha, importe y divisa.

Cuando contacta con nosotros

Cuando se pone en contacto con nosotros a través del chat de atención al cliente o por cualquier otro medio, podemos tratar categorías de datos personales como su correo electrónico, número de teléfono, identificador de cliente, idioma y país, así como cualquier información sobre el estado de su cuenta o detalles de sus transacciones, según el problema que usted esté experimentando. También podemos recopilar otra información si decide proporcionárnosla. Le rogamos que no nos facilite ningún dato personal ni documento adicional, ya sea relativo a usted o a otras personas, a menos que lo solicitemos específicamente.

Cuando visita nuestro sitio web

Cuando visita nuestro sitio web, es posible que recopilemos automáticamente algunos datos personales de su dispositivo. Esta información puede incluir su dirección IP, la fecha y hora de la solicitud, la diferencia de zona horaria con respecto a GMT, el idioma y la versión del navegador, la versión o el productor del sistema operativo, información sobre su dispositivo, así como datos sobre la forma en que interactúa con nuestro sitio web (p. ej., de qué sitio web procede, las páginas visitadas y los enlaces en los que ha hecho clic). Lo hacemos para mantener nuestro sitio web seguro y entender quiénes lo visitan y qué páginas encuentran interesantes, y poder así mejorar el sitio y proporcionar contenido relevante. Algunos de estos datos se recogen mediante cookies. Puede encontrar más información sobre estas en nuestro Aviso de cookies (https://vivid.money/en-eu/cookie-notice/).

Analítica

Tratamos los datos personales que nos proporciona, así como los datos creados como resultado del uso que usted hace de nuestra app, con fines analíticos. Por ejemplo, analizamos cómo interactúa con la app para hacerla más intuitiva y fácil de usar, o para entender si nuestros productos y servicios se adaptan a sus necesidades, y poder así realizar los cambios oportunos en caso necesario, ajustar las tarifas y condiciones, y desarrollar nuevos productos y servicios. En ese caso, dichos datos se despojan de los identificadores directos al objeto de proporcionar una capa de protección adicional. Si desea oponerse a este tratamiento, no dude en contactar con nosotros a través de la dirección de correo electrónico privacy@vivid.money.

Marketing directo

Nos pondremos en contacto con usted cuando lo estimemos oportuno para informarle sobre los nuevos productos o servicios que creamos que puedan ser de su interés. Este tipo de actividad se considera marketing directo, y en este caso nos basamos en su consentimiento o en nuestro interés legítimo para tratar sus datos personales con esta finalidad. Si desea retirar su consentimiento u oponerse a este tratamiento, puede desactivar las notificaciones en el centro de preferencias de su app o hacer clic en el enlace «cancelar suscripción» que figura en la parte inferior del correo electrónico que reciba de nosotros.

Categorías especiales de datos

No le pedimos intencionadamente que proporcione información perteneciente a una categoría «especial», como el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos con la finalidad de identificar de forma exclusiva a una persona, datos relativos a la salud, o datos relativos a la vida sexual u orientación sexual.

Sin embargo, puede haber circunstancias en las que los datos de sus transacciones revelen esta información más sensible. Por ejemplo:

- Los pagos por servicios o tratamientos médicos pueden revelar datos relativos a su salud.
- Realizar contribuciones y donaciones a iglesias, ONG, partidos políticos, sindicatos, etc.

puede revelar sus creencias religiosas o filosóficas, o su afiliación política.
- Los pagos a *sex shops* o a ciertos clubes nocturnos pueden revelar información sensible sobre su vida sexual.

Teniendo en cuenta este riesgo, garantizamos que la información de pago se mantenga confidencial, y prohibimos a nuestro personal extraer datos que pertenezcan a categorías especiales.

Con quién compartimos sus datos personales

Con el fin de proporcionarle determinadas funciones y servicios, debemos compartir sus datos personales con socios, proveedores de servicios externos y entidades afines y reguladoras. Estos solo tratan sus datos personales sobre la base de acuerdos de tratamiento de datos y de acuerdo con instrucciones estrictas, que no les permiten utilizar sus datos para ningún otro fin sin notificárselo o pedirle su consentimiento. Aquí están algunas de las categorías de partes con las que podemos compartir sus datos:

- Nuestro banco socio y corresponsable del tratamiento, Solaris
- Empresas que hacen y entregan las tarjetas que le proporcionamos
- Proveedores de informática y almacenamiento en nube como Amazon Web Services
- Plataformas de analítica e inteligencia empresarial como Snowflake, Mode Analytics, Appsflyer y Amplitude
- Empresas que nos ayudan a enviarle mensajes promocionales y relacionados con el servicio, como Amazon SNS
- Proveedores de servicios de pagos
- Pagadores terceros (personas que introducen dinero en su cuenta), y personas a las que usted transfiere dinero
- Proveedores del software que utilizamos para la atención al cliente y el seguimiento de problemas
- Empresas que nos ayudan con la atención al cliente y la asistencia en las operaciones
- Proveedores de pagos móviles como Google Pay y Apple Pay
- Servicios de analítica web
- Cashback partner

Nosotros, nuestros socios y los proveedores de servicios, entre otros, también podemos vernos obligados a compartir sus datos personales con varias instituciones financieras, o con autoridades judiciales o encargadas de la aplicación de la ley, para cumplir con las leyes aplicables, prevenir el fraude, hacer cumplir un acuerdo que hayamos suscrito con usted, o para proteger nuestros derechos, propiedad o seguridad, o los derechos, propiedad o seguridad de nuestros empleados o agentes.

Además, podemos revelar sus datos personales a terceros en los siguientes casos: 1) si usted lo solicita o lo autoriza; 2) para hacer frente a emergencias o desastres naturales; y 3) para

hacer frente a disputas y reclamaciones, o a personas que acrediten tener autoridad legal demostrable para actuar en su nombre.

Si desea recibir información más detallada sobre los terceros con los que compartimos sus datos personales, póngase en contacto con nosotros a través de la dirección de correo electrónico privacy@vivid.money.

Transferencias de datos a terceros países

Algunos de nuestros socios, proveedores de servicios u otras partes a las que transferimos sus datos personales pueden estar ubicados en países de todo el mundo, incluso fuera de la UE o el EEE. Por consiguiente, los datos pueden enviarse a países con leyes de protección de datos diferentes de las de su país de residencia. En tales casos, para garantizar que sus datos personales reciban un nivel de protección comparable, proporcionamos las garantías adecuadas, como decisiones y marcos de adecuación, o cláusulas contractuales tipo aprobadas por la Comisión Europea. Si desea recibir más información sobre las transferencias o garantías, póngase en contacto con nosotros a través de la dirección de correo electrónico privacy@vivid.money.

Toma de decisiones y elaboración de perfiles automatizados

Tratamos sus datos de forma parcialmente automática para evaluar determinados aspectos personales (elaboración de perfiles). Por ejemplo, utilizamos la elaboración de perfiles para prevenir el fraude y para combatir el blanqueo de dinero, la financiación del terrorismo y los delitos de contaminación de activos. Nuestro modelo de monitorización combina información procedente de detalles de transacciones, datos del perfil del cliente y datos de sesión de dispositivo. El método se basa en las tendencias actuales de fraude y las mejores prácticas de VISA , entre otras fuentes. Estas medidas sirven para proteger sus intereses y mantener sus depósitos seguros.

Cuánto tiempo conservamos sus datos

Conservamos sus datos personales durante el tiempo que es necesario hasta alcanzar la finalidad para la que se recogieron, normalmente durante el curso de nuestra relación contractual más cualquier período posterior que exijan las leyes contra el blanqueo de dinero o cualquier otra legislación aplicable, o en caso de litigios judiciales potenciales o en curso. Cuando se alcance la finalidad del tratamiento, pero se nos exija conservar los datos, estos se restringirán y almacenarán en un fichero seguro hasta que puedan eliminarse.

Sus derechos

Las leyes de protección de datos le otorgan derechos para ayudarle a comprender y controlar cómo se utilizan sus datos personales. Le asisten los siguientes derechos:

- Derecho **a ser informado** sobre por qué y cómo estamos tratando sus datos personales: esperamos haberlo logrado al proporcionarle esta Política de Privacidad.
- Derecho **a tener acceso** a sus datos: tiene derecho a preguntarnos si estamos tratando sus datos personales; por qué lo hacemos; en virtud de qué base jurídica; las categorías de sus datos personales; si los datos se envían fuera de la UE; con quién compartimos sus datos; cuánto tiempo los conservamos; y a solicitar una copia de los datos que estamos tratando. Si no encuentra suficiente información en nuestra Política de Privacidad, póngase en contacto con nosotros a través de la dirección de correo electrónico privacy@vivid.money.
- Derecho **a oponerse** a algún tratamiento: para la finalidad de marketing directo, o si el tratamiento se basa en intereses legítimos.
- Derecho **a que se borren sus datos**: también conocido como «derecho al olvido». Puede ejercitar este derecho si: retira su consentimiento y no existe ningún otro interés legítimo en el tratamiento de sus datos; su oposición al tratamiento en virtud de intereses legítimos prevalece sobre nuestros intereses; el tratamiento ya no es necesario; existe una ley que exige la eliminación de los datos; o el tratamiento es ilícito.
- Derecho **a restringir el tratamiento**: si los datos personales que estamos tratando son inexactos, si nuestro tratamiento es ilícito, si los datos ya no son necesarios para la finalidad original del tratamiento pero deben conservarse en caso de posibles demandas legales o si usted se ha opuesto al tratamiento llevado a cabo en virtud de intereses legítimos y todavía estamos en el proceso de determinar si existe una necesidad imperiosa de continuar realizando dicho tratamiento.
- Derecho a la **portabilidad de los datos**: puede solicitar los datos que tratamos mediante el uso de un ordenador, facilitados por usted sobre la base del consentimiento o por ser necesario para un contrato.
- Derecho a preguntarnos sobre la **toma de decisiones automatizadas**: tiene derecho a pedirnos que le expliquemos la lógica que implica la toma de cualquier decisión automatizada y que la decisión sea revisada por un ser humano, si esa decisión tiene un efecto sobre sus derechos o libertades.
- Derecho de **rectificación**: si alguno de sus datos personales que tenemos es inexacto, puede solicitar que se corrija.
- Tiene **derecho a presentar una reclamación** ante la autoridad de protección de datos competente, si le preocupa la forma en que tratamos sus datos personales (en este sitio web hay disponible una lista de las autoridades nacionales y regionales de protección de datos). Sin embargo, le agradeceríamos que primero se pusiera en contacto con nosotros y nos diera la oportunidad de resolver el problema.

Si desea ejercitar alguno de estos derechos u obtener más información sobre cómo tratamos sus datos personales, póngase en contacto con nosotros a través de la dirección de correo electrónico privacy@vivid.money. El acceso razonable a sus datos personales se proporcionará sin coste alguno. Si no puede darse acceso en un plazo razonable, le comunicaremos la fecha

en que se facilitará la información. Si por algún motivo no podemos satisfacer su petición, le daremos una explicación del porqué.

Seguridad de su información

Para ayudar a proteger la privacidad de los datos personales que usted proporciona a través del uso de nuestro sitio web o app móvil, mantenemos garantías físicas, técnicas y administrativas. Actualizamos y probamos nuestra tecnología de seguridad de forma continua. Restringimos el acceso a sus datos personales a aquellos empleados que necesitan conocer esa información para prestarle servicios. Además, proporcionamos formación a nuestros empleados sobre la importancia de la confidencialidad y de mantener la privacidad y seguridad de los datos. Nos comprometemos a tomar las medidas disciplinarias adecuadas para hacer cumplir las responsabilidades de protección de datos de nuestros empleados.

Cambios y actualizaciones de esta Política de Privacidad

Dado que nuestra organización y servicios cambian de vez en cuando, esta Política de Privacidad también puede cambiar. Nos reservamos el derecho de modificarla cuando lo estimemos oportuno, por cualquier motivo, sin notificárselo de otro modo que no sea la publicación de la Política de Privacidad modificada en nuestro sitio web o en la app móvil. Es posible que enviemos por correo electrónico recordatorios periódicos de nuestros avisos y condiciones generales, y le notificaremos los cambios materiales que se produzcan en ellos, pero debe consultar nuestro sitio o la app para ver la Política de Privacidad vigente y cualquier cambio que se haya realizado en ella.

Última actualización: 17 de julio 2023