Aviso de ThreatMetrix sobre el tratamiento de datos

Última actualización: 10 de octubre de 2023

Acerca de este Aviso sobre el tratamiento de datos

ThreatMetrix, un servicio de LexisNexis Risk Solutions FL Inc. (“LNRS”, “nosotros” o “nuestro(s)” “nuestra(s)”), ayuda a organizaciones a protegerse contra el fraude en línea y la actividad delictiva, y a autenticar a los usuarios de los servicios en línea. Este Aviso sobre el tratamiento de datos explica cómo LNRS trata osa datos personales como parte de los servicios de ThreatMetrix para nuestros clientes en organizaciones (de forma conjunta, “Clientes” y de forma individual, un “Cliente”). El uso de los servicios de ThreatMetrix se rige por los acuerdos aplicables y la Política de privacidad del LexisNexis Risk Solutions.

Información tratada

Nuestros Clientes deciden qué datos personales de sus clientes y potenciales usuarios (de forma conjunta, “Usuarios” y de forma individual, un “Usuario”) puede recibir el servicio de ThreatMetrix, como nombres, números de teléfono móvil, direcciones de correo electrónico, direcciones postales, información de ubicación, datos de tarjetas de pago y otros datos de titulares de tarjetas, datos de transacciones de comercio electrónico e identificadores de dispositivos. Estos datos se convierten automáticamente en token al recibirlos. Esta conversión en token es una medida de seudonimización que convierte un identificador, como un número de cuenta, en una cadena aleatoria de caracteres llamados token, por ejemplo “dh57rh395jf8j02oj94kt784h”. Los tókenes se utilizan para representar el identificador original, pero no se pueden utilizar para volver a identificar los datos. Seguidamente, los tókenes se emparejan entre los diferentes envíos de los Usuarios a través de la Red de Identidad Digital de LexisNexis y se combinan en un identificador digital único: el “LexID Digital”.

También tratamos datos personales vinculada al LexID Digital de forma seudonimizada, incluidos, entre otros: (i) el número de direcciones de correo electrónico y números de teléfono asociados con los dispositivos conectados a Internet de un Usuario; (ii) actividades y atributos asociados con las direcciones de correo electrónico, direcciones de envío, números de teléfono y direcciones IP de un Usuario; (iii) información sobre la huella digital del dispositivo y actividades asociadas con otros identificadores en línea, contraseñas y números del permiso de conducir que el Cliente haya cifrado antes de facilitarlos a nosotros; (iv) datos de la cuenta del Usuario, actividad e historial de inicio de sesión; e (v) historial de transacciones del Usuario asociado con identificadores con función hash de tarjetas de pago, rastreado en el tiempo, junto con las puntuaciones de riesgo asociadas creadas o utilizadas por nosotros a través del uso de los servicios (conjuntamente, “información de atributos”).

Cuando un Cliente utiliza nuestro servicio BehavioSec, se recogen datos de comportamiento, incluidos los movimientos del ratón, las entradas de la pantalla táctil, la pulsación de teclas y los datos de pulsación de teclas. Los datos de pulsación de teclas pueden enmascararse cuando se recogen, por ejemplo, contraseñas. Los datos de pulsación de teclas, tanto de las teclas enmascaradas como de las desenmascaradas, se suprimirán en un plazo de 24 horas. Los datos recogidos por BehavioSec se utilizan para ofrecer puntuaciones y generar alertas con el objetivo de ayudar a prevenir transacciones fraudulentas y verificar que el usuario sea un humano real.

También podemos tratar categorías similares de datos personales recibidos de parte de las empresas vinculadas de LNRS y proveedores de servicios para mejorar la información predictiva de los datos.

Fines y base jurídica para el tratamiento

Tratamos datos personales para nuestros intereses legítimos y los de nuestros Clientes para fines de:

- verificación de identidad;
- detección, investigación, evaluación, supervisión y prevención del fraude y otros delitos;

- mitigación de riesgos financieros y comerciales; y/o
- cumplimiento de las obligaciones en materia de lucha contra el blanqueo de capitales (AML, por sus siglas en inglés), financiación contra el terrorismo (CTF, por sus siglas en inglés), lucha contra el soborno y la corrupción (ABC) y otras obligaciones legales.

También podemos utilizar datos personales para mejorar nuestros servicios, incluidos la mejora de las capacidades analíticas y el desarrollo de nuevos atributos, modelos y puntuaciones, el análisis de la detección de patrones establecidos y anómalos y el análisis de gráficos.

Destinatarios de la información

Compartimos la información sobre atributos:

- con nuestros Clientes, encargados del tratamiento, subencargados del tratamiento y empresas vinculadas;
- cuando creamos de buena fe que dicha divulgación es necesaria para cumplir con cualquier ley, reglamento, procedimiento judicial u otra obligación legal aplicable; para detectar, investigar y ayudar a prevenir problemas de seguridad, fraudes o problemas técnicos; y/o para proteger los derechos, la propiedad o seguridad de LNRS y de nuestras empresas vinculadas, usuarios, empleados u otros; y
- como parte de una transacción corporativa, como por ejemplo una transferencia de activos o una adquisición por parte de otra empresa o fusión con otra empresa.

Retención de los datos

Retenemos los datos personales solo durante el tiempo que sea necesario para prestar los servicios y realizar las transacciones solicitadas por nuestros Clientes, o para otros fines esenciales, tales como cumplir con nuestras obligaciones legales, mantener registros comerciales y financieros, resolver disputas, mantener la seguridad, detectar y prevenir el fraude y el abuso, y hacer cumplir nuestros acuerdos.

Nuestros Clientes son responsables independientes del tratamiento de los datos personales que recibimos de ellos, y es su obligación como responsables del tratamiento determinar sus propios períodos de retención. Es posible que retengan los datos personales durante más tiempo que nosotros.

Seguridad de los datos

Tanto nuestras prácticas como nuestros procesos se han diseñado para proteger los datos que tratamos contra la destrucción, pérdida, alteración, divulgación o el acceso no autorizados, accidentales o ilegales, utilizando medidas de seguridad administrativas, físicas y técnicas adecuadas. Si un Cliente decide enviarnos datos del titular de la tarjeta, somos responsables de tratar dichos datos en nombre del Cliente de acuerdo con la Norma de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS, por sus siglas en inglés).

Elaboración de perfiles

Utilizamos datos personales, como la información de atributos, la ubicación geográfica, las propiedades de red y datos de comportamiento del usuario, enviada por nuestros Clientes para producir diversas puntuaciones. Algunos de estos datos son recogidos por nuestros Clientes y nos los transmiten a través de cookies de ThreatMetrix y tecnologías similares que nuestros Clientes colocan o ejecutan en los dispositivos de sus Usuarios.

Nuestros Clientes pueden utilizar nuestras puntuaciones para predecir el riesgo asociado con una transacción determinada. Las puntuaciones de confianza baja pueden sugerir que las credenciales de identidad se están utilizando de forma fraudulenta o fuera del contexto previo. Las puntuaciones de confianza baja detectan comportamientos inusuales, como anomalías de la ubicación, un número anormalmente alto de nuevas direcciones de correo electrónico que se originan desde el mismo dispositivo o nuevas direcciones de envío que no se han visto antes.

Nuestros Clientes configuran el uso que hacen de nuestros servicios para abordar sus necesidades únicas, lo que puede dar lugar a diferentes puntuaciones entre diferentes Clientes. Nuestros servicios proporcionan una plataforma para tratar y aplicar normas a los datos, pero no recomiendan a nuestros Clientes si deben tomar medidas basadas en las puntuaciones. Para los Usuarios, esto significa que los Clientes pueden tomar decisiones que pueden afectar a la actividad en línea, como prohibir el acceso a un sitio web, permitir que se realice una transacción en línea o exigir a un Usuario que proporcione datos de autenticación adicionales. No tomamos ninguna decisión sobre personas físicas. Dichas decisiones siguen siendo responsabilidad de nuestros Clientes.

Ubicaciones del tratamiento

Tratamos datos personales en los lugares en los que LNRS, sus empresas vinculadas y sus proveedores de servicios mantienen servidores e instalaciones, incluido en Islandia, India, Países Bajos, Reino Unido y Estados Unidos. Tomamos medidas, incluso mediante contratos, destinadas a garantizar que los datos personales sigan estando protegidos dondequiera que se encuentren de manera coherente con los estándares de protección requeridos por la legislación aplicable.

Ciertas entidades de EE.UU. dentro del grupo de empresas de LexisNexis Risk Solutions han certificado algunos de sus servicios conforme al Marco de Privacidad de Datos UE-EE.UU. (EU-U.S. DPF), la Extensión del Reino Unido al EU-U.S. DPF, y el Marco de Privacidad de Datos Suiza-EE.UU. establecidos por el Departamento de Comercio de EE.UU. Consulte el Aviso del Marco de Privacidad de Datos de estas entidades aquí. Para obtener más información sobre el Marco de Privacidad de Datos, y para ver la certificación de estas entidades, visite https://www.dataprivacyframework.gov.

Sus derechos

Conforme a la legislación europea y otras leyes en materia de privacidad y protección de datos, según proceda, usted tiene derecho a solicitar sin cargo alguno:

- el acceso a sus datos personales, así como la corrección o supresión de dicha información;
- la restricción del tratamiento que hacemos de sus datos personales;
- oponerse a nuestro tratamiento; y
- la portabilidad de sus datos personales.

Si desea ejercer cualquiera de estos derechos, póngase en contacto con nosotros en la dirección que figura más abajo. Responderemos a su solicitud de conformidad con las leyes aplicables. Para proteger su privacidad y seguridad, es posible que le pidamos que verifique su identidad. Cuando actuemos como encargados del tratamiento en nombre de nuestro Cliente, le redirigiremos para que realice su solicitud directamente a nuestro Cliente.

Cambios

Actualizaremos este aviso sobre el tratamiento de datos de manera oportuna. Cualquier cambio se publicará en esta página con la fecha de revisión actualizada. Si realizamos algún cambio sustancial, lo notificaremos a través de los servicios o por otros medios.

Contacto

Si tiene alguna pregunta, comentario, queja o solicitud en relación con este aviso sobre el tratamiento de datos, póngase en contacto con nosotros en línea aquí para solicitudes en los EE. UU. o aquí para solicitudes fuera de los EE. UU. O si lo prefiere puede escribir a: Delegado de protección de datos, LexisNexis Risk Solutions, Global Reach, Dunleavy Drive, Cardiff CF11 0SN, Reino Unidomailto:. También puede presentar una reclamación ante la autoridad de protección de datos en la jurisdicción correspondiente.