Verarbeitungshinweis zu ThreatMetrix

Zuletzt aktualisiert: 10. Oktober 2023

Über diesen Verarbeitungshinweis

ThreatMetrix, ein Dienst der LexisNexis Risk Solutions FL Inc. („LNRS“, „wir“ oder „unser“), unterstützt Unternehmen beim Schutz vor Online-Betrug und -Kriminalität sowie bei der Authentifizierung der Nutzer von Online-Diensten. In diesem Verarbeitungshinweis wird erläutert, wie LNRS für unsere Unternehmenskunden (zusammen als „Kunden“ und jeweils einzeln als „Kunde“ bezeichnet) personenbezogene Daten mittels der ThreatMetrix-Dienste verarbeitet. Die Nutzung der ThreatMetrix-Dienste unterliegt den geltenden Vereinbarungen und der Datenschutzrichtlinie der LexisNexis Risk Solutions.

Verarbeitete Informationen

Es liegt im Ermessen unserer Kunden, welche personenbezogenen Daten ihrer aktuellen und potenziellen Endkunden (zusammen als „Endkunden“ und jeweils einzeln als „Endkunde“ bezeichnet) ThreatMetrix erhalten darf, wie z. B. Namen, Mobiltelefonnummern, E-Mail-Adressen, Postanschriften, Standortinformationen, Zahlungskarten- und andere Karteninhaberdaten, E-Commerce-Transaktionsdaten und Gerätekennungen. Diese Daten werden beim Empfang automatisch tokenisiert. Eine Tokenisierung ist eine Art der Pseudonymisierung, bei der eine Kennung, wie z. B. eine Kontonummer, in einen „Token“, d. h. eine zufällige Zeichenfolge, z. B. „dh57rh395jf8j02oj94kt784h“ umwandelt wird. Tokens dienen der bildlichen Darstellung der ursprünglichen Kennung, können jedoch nicht dazu verwendet werden, die Daten erneut zu identifizieren. Die Tokens werden dann über verschiedene Kundeneingaben im gesamten LexisNexis Digital Identity Network hinweg miteinander abgeglichen und zu einer eindeutigen digitalen Kennung kombiniert: der „LexID Digital“.

Wir verarbeiten personenbezogene Daten, die mit der LexID Digital verknüpft sind, auch in pseudonymisierter Form, einschließlich u. a.: (i) die Anzahl der E-Mail-Adressen und Telefonnummern, die mit den internetfähigen Geräten eines Endkunden verknüpft sind; (ii) Aktivitäten und Attribute, die mit den E-Mail-Adressen, Versandadressen, Telefonnummern und IP-Adressen eines Endkunden verknüpft sind; (iii) Device-Fingerprinting-Informationen und Aktivitäten, die mit anderen Online-IDs, Passwörtern und Führerscheinnummern verknüpft sind, die vom Kunden vor der Übermittlung an uns gehasht wurden; (iv) Kontodaten, Anmeldeaktivität und -verlauf von Endkunden; und (v) Transaktionsverlauf von Endkunden, der mit gehashten Zahlungskartenkennungen verknüpft ist, im Laufe der Zeit, zusammen mit den damit verbundenen Risikowerten, die von uns mittels der Dienste erstellt oder angewandt werden (zusammen als „Attributinformationen“ bezeichnet).

Unser BehavioSec-Dienst erhebt bei der Nutzung durch Kunden Verhaltensdaten, einschließlich Mausbewegungen, Touchscreen-Eingaben, Tastenanschlägen und Tastendruckdaten. Tastendruckdaten, z. B. Passwörter, können bei Erhebung maskiert werden. Sowohl maskierte als auch nicht maskierte Tastendruckdaten werden innerhalb von 24 Stunden gelöscht. Die von BehavioSec erhobenen Daten werden zur Erstellung von Werten und zur Auslösung von Warnungen genutzt, die betrügerische Transaktionen verhindern und überprüfen sollen, ob es sich bei dem Nutzer um einen echten Menschen handelt.

Ähnliche Kategorien personenbezogener Daten, die wir von verbundenen Unternehmen und Dienstleistern von LNRS erhalten, können von uns zur Verbesserung der Vorhersageerkenntnisse bezüglich Daten verarbeitet werden.

Zwecke und Rechtsgrundlage der Verarbeitung

Wir verarbeiten personenbezogene Daten zur Wahrnehmung unserer eigenen berechtigten Interessen und der unseren Kunden zu folgenden Zwecken:

- Überprüfung der Identität;
- Aufdeckung, Untersuchung, Quantifizierung, Überwachung und Prävention von Betrug und anderen Straftaten;
- Minderung finanzieller und geschäftlicher Risiken; und/oder
- Einhaltung von Gesetzen zur Bekämpfung von Geldwäsche (Anti-Money Laundering, AML), Terrorismusfinanzierung (Counter-Terrorism Financing, CTF), Bestechung und Korruption (Anti-Bribery and Corruption, ABC) und anderen rechtlichen Verpflichtungen.

Wir können personenbezogene Daten auch zur Verbesserung unserer Dienste nutzen, einschließlich der Verfeinerung von Analysefähigkeiten und der Entwicklung neuer Attribute, Modelle und Werte, der Analyse etablierter und anomaler Mustererkennung und der Diagrammanalyse.

Empfänger der Informationen

Wir geben Attributinformationen wie folgt weiter:

- an unsere Kunden, Auftragsverarbeiter, Auftragsverarbeiter im Unterauftragsverhältnis und verbundenen Unternehmen;
- wenn wir in gutem Glauben der Ansicht sind, dass eine solche Offenlegung erforderlich ist, um geltende Gesetze, Vorschriften, rechtliche Verfahren oder andere rechtliche Verpflichtungen zu erfüllen, Sicherheits-, Betrugs- oder technische Probleme aufzudecken, zu untersuchen und zu verhindern und/oder die Rechte, das Eigentum oder die Sicherheit von LNRS und unseren verbundenen Unternehmen, Nutzern, Mitarbeitern oder anderen zu schützen; und
- im Rahmen einer Unternehmenstransaktion, wie z. B. einer Übertragung von Vermögenswerten oder einer Übernahme durch ein anderes Unternehmen bzw. einer Fusion mit einem anderen Unternehmen.

Aufbewahrung von Daten

Wir bewahren personenbezogene Daten nur so lange auf, wie dies für die Bereitstellung der Dienste bzw. Bearbeitung der Transaktionen, die von unseren Kunden angefordert werden, oder für andere wesentliche Zwecke erforderlich ist, wie z. B. die Erfüllung unserer gesetzlichen Verpflichtungen, die Führung von Geschäfts- und Finanzbüchern, die Beilegung von Streitigkeiten, die Aufrechterhaltung der Sicherheit, die Aufdeckung und Prävention von Betrug und Missbrauch sowie die Durchsetzung unserer Vereinbarungen.

Unsere Kunden gelten für personenbezogene Daten, die wir von ihnen erhalten, als separate Verantwortliche und sind als solche verpflichtet, ihre eigenen Aufbewahrungsfristen festzulegen. Diese bewahren personenbezogene Daten möglicherweise länger auf als wir.

Datensicherheit

Unsere Methoden und Verfahren dienen dem Schutz der von uns verarbeiteten Daten vor versehentlicher oder rechtswidriger Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder Zugriff. Erreicht wird dies durch Umsetzung geeigneter administrativer, physischer und technischer Sicherheitsmaßnahmen. Werden uns von Kunden Karteninhaberdaten übermittelt, sind wir für die Verarbeitung dieser Daten im Auftrag des Kunden in Übereinstimmung mit dem Payment Card Industry Data Security Standard (PCI DSS) verantwortlich.

Profiling

Wir nutzen personenbezogene Daten wie Attributinformationen, geografischer Standort, Netzwerkeigenschaften und Nutzerverhaltensdaten, die wir von unseren Kunden erhalten, zur Erstellung diverser Werte. Einige dieser Daten werden von unseren Kunden erhoben und über Cookies und ähnliche Technologien von ThreatMetrix, die unsere Kunden auf den Geräten ihrer Endkunden platzieren oder ausführen, an uns weitergegeben.

Unsere Werte können von unseren Kunden zur Prognose des mit einer bestimmten Transaktion verbundenen Risikos verwendet werden. Niedrige Vertrauenswerte können darauf hindeuten, dass Identitäts-/Anmeldedaten in betrügerischer Weise verwendet/zweckentfremdet werden. Durch niedrige Vertrauenswerte kann außerdem ungewöhnliches Verhalten erkannt werden, wie z. B. Standortanomalien, ungewöhnlich hohe Anzahl neuer E-Mail-Adressen, die von demselben Gerät stammen, oder bisher unbekannte neue Versandadressen.

Unsere Kunden konfigurieren unsere Dienste entsprechend ihren individuellen Bedürfnissen, was zu Unterschieden bei den zugewiesenen Werten führen kann. Wir bieten im Rahmen unserer Dienste eine Plattform für die Verarbeitung und Anwendung von Regeln auf Daten an, empfehlen unseren Kunden jedoch nicht, die Werte als Grundlage für irgendwelche Maßnahmen heranzuziehen. Für die Endkunden bedeutet dies, dass unsere Kunden Entscheidungen treffen können, die sich möglicherweise auf ihre Online-Aktivitäten auswirken, wie z. B. eine Zugriffssperre für eine Website, die Genehmigung einer Online-Transaktion oder die Aufforderung zur Bereitstellung zusätzlicher Authentifizierungsdaten. Wir selbst treffen keine Entscheidungen mit Auswirkungen auf Einzelpersonen. Dies obliegt nach wie vor unseren Kunden.

Standorte der Verarbeitung

Wir verarbeiten personenbezogene Daten an den Standorten, an denen LNRS, seine verbundenen Unternehmen und ihre Dienstleister über Server oder Anlagen verfügen, einschließlich in Island, Indien, den Niederlanden, dem Vereinigten Königreich und den Vereinigten Staaten. Wir ergreifen Maßnahmen, einschließlich durch Verträge, um sicherzustellen, dass die personenbezogenen Daten unabhängig vom Standort ihrer Aufbewahrung weiterhin gemäß den nach geltendem Recht erforderlichen Schutzstandards geschützt bleiben.

Einige US-Unternehmen innerhalb der LexisNexis Risk Solutions Unternehmensgruppe haben bestimmte ihrer Dienstleistungen unter den Datenschutzrahmen EU-USA (EU-U.S. DPF), das Vereinigte Königreich Erweiterung des EU-U.S. DPF und Datenschutzrahmen Swiss-U.S. zertifizieren lassen, wie vom US-Handelsministerium festgelegt. Bitte beachten Sie den Datenschutzrahmen Hinweis dieser Unternehmen hier. Um mehr über das Datenschutzrahmen zu erfahren und die Zertifizierung dieser Unternehmen anzusehen, besuchen Sie bitte https://www.dataprivacyframework.gov.

Ihre Rechte

Sie haben gemäß den europäischen und bestimmten anderen Datenschutzgesetzen das Recht, Folgendes kostenlos anzufordern bzw. zu erheben:

- Zugriff auf Ihre personenbezogenen Daten, Korrektur oder Löschung dieser;
- Einschränkung unserer Verarbeitung Ihrer personenbezogenen Daten;
- Widerspruch gegen unsere Verarbeitung; und
- Übertragbarkeit Ihrer personenbezogenen Daten.

Wenn Sie eines dieser Rechte ausüben möchten, kontaktieren Sie uns bitte unter der unten angegebenen Adresse. Wir beantworten Ihre Anfrage in Übereinstimmung mit den geltenden Gesetzen. Zum Schutz Ihrer Privatsphäre und Sicherheit können wir Sie um einen Nachweis Ihrer Identität bitten. Wenn wir im Auftrag eines unserer Kunden als Auftragsverarbeiter handeln, verweisen wir Sie für die Übermittlung von Anfragen direkt an unseren Kunden.

Änderungen

Wir können diesen Verarbeitungshinweis von Zeit zu Zeit aktualisieren. Änderungen werden auf dieser Seite veröffentlicht, zusammen mit einem aktualisierten Überarbeitungsdatum. Sollten wir wesentliche Änderungen vornehmen, werden wir Sie darüber über die Dienste oder auf andere Weise informieren.

Kontakt

Kontaktieren Sie uns bei Fragen, Anmerkungen, Beschwerden oder Anfragen zu diesem Verarbeitungshinweis bitte online hier, falls Sie in den USA ansässig sind, oder hier, falls Sie außerhalb der USA ansässig sind. Alternativ können Sie uns wie folgt postalisch kontaktieren: Data Protection Officer (Datenschutzbeauftragte(r)), LexisNexis Risk Solutions, Global Reach, Dunleavy Drive, Cardiff CF11 0SN, Vereinigtes Königreichmailto:. Ferner können Sie ggf. Beschwerde bei der Datenschutzbehörde im relevanten Land erheben.