Kennisgeving van verwerking van ThreatMetrix

Laatst bijgewerkt: 10 oktober 2023

Over deze kennisgeving van verwerking

ThreatMetrix, een dienst van LexisNexis Risk Solutions FL Inc.(“LNRS, “wij/we” of “ons/onze”), helpt organisaties te beschermen tegen online fraude en criminele activiteiten en om gebruikers van online diensten te verifiëren. In deze verwerkingskennisgeving wordt uitgelegd hoe LNRS persoonlijke informatie verwerkt als onderdeel van de ThreatMetrix-diensten voor onze organisatorische klanten (gezamenlijk “Klanten” en elk een “Klant”). Het gebruik van de ThreatMetrix-diensten wordt beheerst door de toepasselijke overeenkomsten en het Privacybeleid van de LexisNexis Risk Solutions .

Verwerkte Informatie

Onze Klanten kiezen welke persoonlijke informatie van hun cliënten en potentiële cliënten (gezamenlijk “Cliënten” en elk een “Cliënt”) de ThreatMetrix-dienst bevoegd is te ontvangen, zoals namen, mobiele telefoonnummers, e-mailadressen, postadressen, locatiegegevens, betaalkaart- en andere kaarthoudergegevens, transactiegegevens van e-commerce en apparaat-ID’s. Deze gegevens worden na ontvangst automatisch getokeniseerd. Tokenisatie is een pseudonimiseringsmaatregel die een identificatiemiddel, zoals een rekeningnummer, omzet in een willekeurige reeks tekens die een token wordt genoemd, bijvoorbeeld ‘dh57rh395jf8j02oj94kt784h’. Tokens worden gebruikt om het oorspronkelijke identificatiemiddel te vertegenwoordigen, maar kunnen niet worden gebruikt om de gegevens opnieuw te identificeren. De tokens worden vervolgens gekoppeld aan de inzendingen van verschillende Klanten in het LexisNexis Digital Identity Network en gecombineerd tot een uniek digitaal identificatiemiddel: de “LexID Digital”.

We verwerken ook persoonlijke informatie gekoppeld aan de LexID Digital in een pseudonieme vorm, waaronder, maar niet beperkt tot: (i) het aantal e-mailadressen en telefoonnummers dat is gekoppeld aan de met internet verbonden apparaten van een Cliënt; (ii) activiteiten en kenmerken die verband houden met de e-mailadressen, verzendadressen, telefoonnummers en IP-adressen van een Cliënt; (iii) vingerafdrukgegevens van een apparaat en activiteiten in samenhang met andere online ID’s, wachtwoorden en rijbewijsnummers, die door de Klant zijn gehasht voordat ze aan ons zijn verstrekt; (iv) Gegevens van de rekening, inlogactiviteit en geschiedenis van de Cliënt; en (v) transactiegeschiedenis van de Cliënt geassocieerd met gehashte betaalkaartidentificatiemiddelen, in de loop van de tijd gevolgd, samen met de bijbehorende risicoscores die door ons zijn gecreëerd of gebruikt door het gebruik van de diensten (gezamenlijk “attribuutinformatie”).

Wanneer een Klant gebruikmaakt van onze BehavioSec-dienst, worden gedragsgegevens, waaronder muisbewegingen, touchscreeninvoer en toetsaanslaggegevens verzameld. Toetsaanslaggegevens kunnen worden gemaskeerd wanneer ze worden verzameld, bijvoorbeeld wachtwoorden. Zowel de gemaskeerde als de niet-gemaskeerde toetsaanslaggegevens worden binnen 24 uur verwijderd. De gegevens die door BehavioSec worden verzameld, worden gebruikt om scores te produceren en waarschuwingen te genereren om frauduleuze transacties te helpen voorkomen en te verifiëren dat de gebruiker een echt mens is.

We kunnen ook soortgelijke categorieën persoonlijke informatie verwerken die we ontvangen van aan LNRS gelieerde bedrijven en dienstverleners om de voorspellende inzichten van gegevens te verbeteren.

Doeleinden en rechtsgrond voor verwerking

We verwerken persoonlijke informatie voor de legitieme belangen van ons en onze Klanten voor:

- identiteitsverificatie;
- opsporing, onderzoeken, beoordeling, controle en voorkoming van fraude en andere criminaliteit;
- beperking van financiële en zakelijke risico’s; en/of
- naleving van anti-witwaspraktijken (Anti-Money Laundering, AML), financiering van terrorismebestrijding (Counter-Terrorism Financing, CTF), anti-omkoping en -corruptie (Anti-Bribery and Corruption, ABC) en andere wettelijke verplichtingen.

We kunnen ook persoonlijke informatie gebruiken voor de verbetering van onze diensten, waaronder het verfijnen van analysemogelijkheden en de ontwikkeling van nieuwe attributen, modellen en scores, het analyseren van vastgestelde en afwijkende patroondetectie en grafiekanalyse.

Ontvangers van Informatie

We delen attribuutinformatie:

- met onze Klanten, verwerkers, subverwerkers en gelieerde bedrijven;
- wanneer wij te goeder trouw geloven dat een dergelijke vrijgave noodzakelijk is om te voldoen aan alle toepasselijke wet- en regelgeving, gerechtelijke procedures of andere wettelijke verplichtingen; om beveiligings-, fraude- of technische problemen op te sporen, te onderzoeken en te helpen voorkomen; en/of om de rechten, eigendommen of veiligheid van LNRS en onze gelieerde bedrijven, gebruikers, medewerkers of anderen te beschermen; en
- in het kader van een zakelijke transactie, zoals een overdracht van activa aan of een overname door of fusie met een andere vennootschap.

Gegevensbewaring

Wij bewaren persoonlijke informatie slechts zo lang als nodig is om de diensten te verlenen en de transacties uit te voeren waarom onze Klanten hebben verzocht, of voor andere essentiële doeleinden, zoals het voldoen aan onze wettelijke verplichtingen, het bijhouden van zakelijke en financiële gegevens, het oplossen van geschillen, het handhaven van de veiligheid, het opsporen en voorkomen van fraude en misbruik, en het afdwingen van onze overeenkomsten.

Onze Klanten zijn afzonderlijke verwerkingsverantwoordelijken voor de persoonlijke informatie die we van hen ontvangen, en het is hun verplichting als verwerkingsverantwoordelijken om hun eigen bewaartermijnen te bepalen. Zij bewaren persoonlijke informatie wellicht langer dan wij.

Gegevensbeveiliging

Onze praktijken en processen zijn ontworpen om de gegevens die we verwerken, te beschermen tegen onopzettelijk(e) of onwettig(e) vernietiging, verlies, wijziging, ongeoorloofde openbaarmaking of toegang, met behulp van passende administratieve, fysieke en technische beveiligingsmaatregelen. Als een Klant ervoor kiest om ons kaarthoudergegevens te sturen, zijn wij verantwoordelijk voor het verwerken van dergelijke gegevens namens de Klant in overeenstemming met de Payment Card Industry Data Security Standard (PCI DSS).

Profilering

We gebruiken persoonlijke informatie, zoals attribuutinformatie, geografische locatie, netwerkeigenschappen en gegevens over gebruikersgedrag, die door onze Klanten worden verzonden, om verschillende scores te produceren. Sommige van deze gegevens worden door onze Klanten verzameld en aan ons doorgegeven via ThreatMetrix-cookies en soortgelijke technologieën die onze Klanten op de apparaten van hun Cliënten plaatsen of gebruiken.

Onze scores kunnen door onze Klanten worden gebruikt om het risico te voorspellen dat aan een bepaalde transactie is verbonden. Lage betrouwbaarheidsscores kunnen suggereren dat identiteitsaanmeldgegevens frauduleus/buiten eerdere context worden gebruikt. Lage vertrouwensscores detecteren ongewoon gedrag, zoals locatieafwijkingen, een abnormaal hoog aantal nieuwe e-mailadressen afkomstig van hetzelfde apparaat of nieuwe verzendadressen die nog niet eerder zijn gezien.

Onze Klanten configureren hun gebruik van onze diensten om aan hun unieke behoeften te voldoen, wat kan leiden tot verschillende scores onder verschillende Klanten. Onze diensten bieden een platform voor het verwerken en toepassen van regels op gegevens, maar raden onze Klanten niet aan om al dan niet actie te ondernemen op basis van scores. Voor de Cliënten betekent dit dat Klanten beslissingen kunnen nemen die van invloed kunnen zijn op online activiteiten, zoals het verbieden van toegang tot een website, het toestaan van een online transactie of van een Cliënt aanvullende verificatiegegevens eisen. We nemen geen beslissingen over een individu. Dergelijke beslissingen blijven voor onze Klanten.

Locaties van verwerking

Wij verwerken persoonlijke informatie waar LNRS, haar gelieerde bedrijven en hun dienstverleners servers en faciliteiten onderhouden, waaronder in IJsland, India, Nederland, het Verenigd Koninkrijk en de Verenigde Staten. Wij nemen maatregelen, onder meer door middel van contracten, om ervoor te zorgen dat de persoonlijke informatie beschermd blijft, waar deze zich ook bevindt, op een manier die in overeenstemming is met de beschermingsnormen die door de toepasselijke wetgeving worden vereist.

Bepaalde Amerikaanse entiteiten binnen de LexisNexis Risk Solutions groepsbedrijven hebben enkele van hun diensten gecertificeerd onder het EU-VS-kader voor gegevensbescherming ("EU-U.S. DPF"), de Britse uitbreiding naar het EU-U.S. DPF en het Zwitserland-VS-kader voor gegevensbescherming op de wijze als bepaald door het Amerikaanse Ministerie van Handel. U vindt het kader voor gegevensbescherming Notice hier. Voor meer informatie over het kader voor gegevensbescherming en om de certificering van deze bedrijven in te zien gaat u naar https://www.dataprivacyframework.gov.

Uw rechten

U hebt op grond van Europese en bepaalde andere privacy- en gegevensbeschermingswetten, voor zover van toepassing, het recht om kosteloos een verzoek in te dienen om:

- toegang tot en correctie of verwijdering van uw persoonlijke informatie;
- beperking van onze verwerking van uw persoonlijke informatie;
- het maken van bezwaar tegen onze verwerking; en
- overdraagbaarheid van uw persoonlijke informatie.

Als u een van deze rechten wilt uitoefenen, neem dan contact met ons op via het onderstaande adres. We zullen op uw verzoek reageren in overeenstemming met de toepasselijke wetgeving. Om uw privacy en beveiliging te beschermen, kunnen wij u mogelijk vragen uw identiteit bevestigen. Wanneer we namens onze Klant optreden als verwerker, zullen we u doorverwijzen om uw verzoek rechtstreeks aan onze Klant te doen.

Wijzigingen

We zullen deze verwerkingskennisgeving van tijd tot tijd bijwerken. Eventuele wijzigingen zullen op deze pagina worden geplaatst met een bijgewerkte herzieningsdatum. Als we materiële wijzigingen aanbrengen, zullen we u op de hoogte stellen via de diensten of op een andere manier.

Contact

Als u vragen, opmerkingen, klachten of verzoeken hebt met betrekking tot deze kennisgeving van verwerking, neem dan hier online contact met ons op voor verzoeken in de VS of hier voor verzoeken buiten de VS. U kunt ook schrijven naar: Data Protection Officer, LexisNexis Risk Solutions, Global Reach, Dunleavy Drive, Cardiff CF11 0SN, Verenigd Koninkrijkmailto:. U kunt ook een klacht indienen bij de gegevensbeschermingsautoriteit in het toepasselijke rechtsgebied.