Notice d’information relative au traitement des données de ThreatMetrix

Dernière mise à jour : 10 octobre 2023

À propos de cette notice d’information relative au traitement des données

ThreatMetrix, un service de la société LexisNexis Risk Solutions FL Inc. (« LNRS », « nous », « notre » ou « nos ») permet aux organisations de se protéger contre la fraude et les activités criminelles en ligne, et d’authentifier les utilisateurs de services en ligne. La présente notice d’information relative au traitement des données décrit comment LNRS traite les données à caractère personnel dans le cadre des services ThreatMetrix pour ses clients professionnels (collectivement, les « Clients » et chacun, un « Client »). L’utilisation des services ThreatMetrix est régie par les contrats applicables et la Politique de confidentialité du LexisNexis Risk Solutions.

Données traitées

Nos Clients sélectionnent les données à caractère personnel de leurs utilisateurs et utilisateurs potentiels (collectivement, les « Utilisateurs » et chacun, un « Utilisateur ») que le service ThreatMetrix est autorisé à recevoir, telles que les noms, les numéros de téléphone portable, les adresses e-mail, les adresses postales, les informations de localisation, les données de cartes de paiement et autres données du titulaire de la carte, les données de transaction d’e-commerce et les identifiants de l’appareil. Ces données sont automatiquement tokenisées dès leur réception. La tokenisation est une mesure de pseudonymisation qui transforme un identifiant, tel qu’un numéro de compte, en une chaîne de caractères aléatoires appelée token, par exemple « dh57rh395jf8j02oj94kt784h ». Les tokens sont utilisés pour représenter l’identifiant d’origine, mais ne peuvent pas servir à réidentifier les données. Les tokens sont ensuite reliés entre les différentes soumissions des Clients sur l’ensemble du réseau d’identités numériques de LexisNexis et combinés en un identifiant numérique unique : le « LexID Digital ».

Nous traitons également les données à caractère personnel liées au LexID Digital sous forme pseudonyme, y compris, mais sans s’y limiter : (i) le nombre d’adresses e-mail et de numéros de téléphone associés aux appareils connectés à Internet d’un Utilisateur ; (ii) les activités et attributs associés aux adresses e-mail, adresses de livraison, numéros de téléphone, adresses IP d’un Utilisateur ; (iii) les informations d’empreintes digitales de l’appareil et les activités associées à d’autres identifiants en ligne, mots de passe et numéros de permis de conduire, qui ont été hachées par le Client avant de nous être communiquées ; (iv) les détails du compte, l’activité et historique de connexion de l’Utilisateur ; et (v) l’historique des transactions de l’Utilisateur associé à des identifiants de carte de paiement hachés, suivis au fil du temps, ainsi que les scores de risque associés créés ou utilisés par nous dans le cadre de l’utilisation des services (collectivement, les « informations d’attributs »).

Lorsqu’un Client utilise notre service BehavioSec, des données comportementales sont collectées, notamment les déplacements de la souris, les actions sur l’écran tactile, les données relatives aux frappes sur le clavier et aux touches utilisées. Les données relatives aux touches utilisées peuvent être masquées lorsqu’elles sont collectées, notamment lors de la saisie des mots de passe. Les données relatives aux touches utilisées qui sont masquées ou non sont supprimées dans les 24 heures. Les données collectées par BehavioSec sont utilisées pour produire des scores et générer des alertes afin d’aider à prévenir les transactions frauduleuses et de vérifier que l’utilisateur est bien un être humain.

Nous pouvons également traiter des catégories similaires de données à caractère personnel reçues des sociétés affiliées et des prestataires de services de LNRS afin d’améliorer l’analyse prédictive des données.

Finalités et base juridique du traitement

Nous traitons les données à caractère personnel pour nos intérêts légitimes et ceux de nos Clients pour :

- la vérification de l'identité ;
- la détection, l'évaluation, le contrôle et la prévention de la fraude et d'autres délits, et les enquêtes ;
- l'atténuation des risques financiers et commerciaux ; et/ou
- le respect des obligations en matière de lutte contre le blanchiment d'argent (AML), de lutte contre le financement du terrorisme (CFT), de lutte contre la corruption (ABC) et d'autres obligations légales.

Nous pouvons également utiliser les données à caractère personnel pour améliorer nos services, notamment en perfectionnant les capacités d'analyse et en développant de nouveaux attributs, modèles et scores, en étudiant les modèles établis et anormaux de détection et en procédant à des analyses graphiques.

Destinataires des données

Nous partageons des données relatives aux attributs :

- avec nos Clients, sous-traitants, sous-traitants ultérieurs et sociétés affiliées ;
- lorsque nous estimons de bonne foi qu'une telle divulgation est nécessaire pour se conformer à une loi, une réglementation, une procédure judiciaire ou à une autre obligation légale applicable ; pour détecter les problèmes de sécurité, de fraude ou techniques, aider à les prévenir et enquêter ; et/ou pour protéger les droits, les biens ou la sécurité de LNRS et de ses sociétés affiliées, utilisateurs, employés ou autres ; et
- dans le cadre d'une transaction générale, telle qu'un transfert d'avoirs ou une acquisition par le biais d'une fusion avec une autre société.

Conservation des données

Nous ne conservons les données à caractère personnel que pendant la durée nécessaire pour fournir les services et remplir les transactions demandées par nos Clients, ou à d'autres finalités essentielles, telles que le respect de nos obligations légales, la tenue d'archives commerciales et financières, le règlement de différends, le maintien de la sécurité, la détection et la prévention de la fraude et d'abus, et l'application de nos contrats.

Nos Clients sont eux-mêmes les responsables du traitement des données à caractère personnel que nous recevons de leur part, et il leur incombe, en tant que responsables du traitement, de fixer leurs propres durées de conservation. Il est possible que leur durée de conservation des données soit plus longue que la nôtre.

Sécurité des données

Nos pratiques et processus sont conçus pour protéger les données que nous traitons contre la destruction fortuite ou illicite, la perte, la modification, la divulgation ou l'accès non autorisé en utilisant des mesures de sécurité administratives, physiques et techniques appropriées. Si un Client décide de nous envoyer des données de titulaires de carte, nous sommes responsables du traitement de ces données pour le compte du Client conformément à la Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS).

Profilage

Nous utilisons les données à caractère personnel, telles que les données relatives aux attributs, la localisation géographique, les propriétés du réseau et les données de comportement des utilisateurs, envoyées par nos Clients afin de produire divers scores. Certaines de ces données sont collectées par nos Clients et nous sont transmises par le biais de cookies ThreatMetrix et de technologies similaires que nos Clients déposent ou utilisent sur les appareils de leurs Utilisateurs.

Nos scores peuvent être utilisés par nos Clients pour prédire le risque associé à une transaction donnée. Des scores de confiance faibles peuvent suggérer que les identifiants d'identité sont utilisés frauduleusement ou hors contexte antérieur. Les scores de confiance faibles détectent les comportements inhabituels, comme les anomalies de localisation, un nombre anormalement élevé de nouvelles adresses e-

mail provenant d'un même appareil ou de nouvelles adresses d'expédition qui n'ont jamais été vues auparavant.

Nos Clients configurent leur utilisation de nos services pour répondre à leurs besoins uniques, les scores peuvent donc varier d'un Client à l'autre. Nos services fournissent une plateforme de traitement et d'application de règles aux données, mais ne recommandent pas à nos Clients de prendre des mesures en fonction des scores. Pour les Utilisateurs, cela signifie que les Clients peuvent prendre des décisions susceptibles d'affecter l'activité en ligne, comme interdire l'accès à un site web, autoriser à procéder à une transaction en ligne ou demander à un Utilisateur de fournir des données d'authentification supplémentaires. Nous ne prenons aucune décision concernant une personne. C'est à nos Clients de prendre ces décisions.

Localisations du Traitement

Nous traitons les données à caractère personnel là où LNRS, ses sociétés affiliées et leurs prestataires de services disposent de serveurs et d'installations, notamment en Islande, en Inde, aux Pays-Bas, au Royaume-Uni et aux États-Unis. Nous prenons des mesures, y compris par le biais de contrats, dont le but est d'assurer que les données à caractère personnel continuent à être protégées là où elles sont localisées en toute cohérence avec les normes de protection imposées par la loi en vigueur.

Certaines entités des États-Unis au sein du groupe de sociétés de LexisNexis Risk Solutions ont certifié certains de leurs services selon le cadre de protection des données UE - États-Unis (EU-U.S. DPF), l'extension du Royaume-Uni au EU-U.S. DPF, et le cadre de protection des données Suisse - États-Unis tel qu'établi par le Ministère du Commerce des États-Unis. Veuillez consulter l'avis relatif au respect du cadre de protection des données de ces entités ici. Pour en savoir plus sur le programme de cadre de protection des données, et pour consulter la certification de ces entités, veuillez visiter https://www.dataprivacyframework.gov.

Vos droits

Vous avez le droit, en vertu des lois européennes et de certaines autres lois relatives à la confidentialité et la protection des données, selon le cas, de demander gratuitement :

- l'accès à vos données à caractère personnel, leur correction ou leur suppression ;
- la limitation du traitement de vos données à caractère personnel ;
- l'opposition au traitement ; et
- la portabilité de vos données à caractère personnel.

Si vous souhaitez exercer l'un de ces droits, veuillez nous contacter à l'adresse ci-dessous. Nous répondrons à votre demande dans le respect des lois en vigueur. Pour protéger votre vie privée et votre sécurité, nous pouvons vous demander de vérifier votre identité. Lorsque nous agissons en tant que sous-traitants pour le compte de notre Client, nous vous inviterons à faire votre demande directement auprès de notre Client.

Modifications

Nous mettrons à jour cette notice d'information relative au traitement des données de temps à autre. Toutes les modifications seront publiées sur cette page avec la date de la dernière révision. En cas de modifications substantielles, nous vous en informerons par le biais des services ou par d'autres moyens.

Contact

Si vous avez des questions, des commentaires, des réclamations ou des demandes concernant cette notice d'information relative au traitement des données, veuillez nous contacter en ligne ici pour les demandes en provenance des États-Unis ou ici pour les demandes en provenance d'autres pays. Vous pouvez également nous contacter par courrier postal à : Délégué à la protection des données, LexisNexis Risk Solutions, Global Reach, Dunleavy Drive, Cardiff CF11 0SN, Royaume-Unimailto:. Vous pouvez également introduire une réclamation auprès de l'autorité de protection des données de la juridiction compétente.