Politique mondiale de protection de la vie privée

La présente Politique de protection de la vie privée explique comment nous traitons les données des personnes utilisant nos services de vérification ou d'authentification. Différentes sections à la fin de la Politique couvrent la manière dont nous traitons les données des candidats à l'emploi et des contacts professionnels.

1. Introduction

La protection de la vie privée est un droit humain fondamental. Vos informations personnelles sont exactement ce qu'elles sont, les vôtres. Chez IDVerse, nous tenons à ce qu'il en soit ainsi. C'est pourquoi la protection de la vie privée est primordiale pour nous, dans tout ce que nous faisons, et nous nous engageons à respecter votre vie privée.

Notre Politique de protection de la vie privée définit la manière dont nous collectons, détenons, utilisons, stockons et divulguons vos informations personnelles et sensibles. Nous pouvons modifier notre Politique de protection de la vie privée au fil du temps, en publiant les modifications sur notre site Internet. Nous vous encourageons à consulter régulièrement notre site Internet pour vous assurer d'être correctement informé de notre Politique de protection de la vie privée la plus à jour.

Aux fins de la présente Politique de protection de la vie privée, « nous », « notre » ou « nos » désigne les différentes entreprises d'IDVerse (reprises à la fin de la présente Politique). Nous sommes tenus à différentes legislations mondiales sur la protection des données en fonction de votre lieu de résidence, dont le GDPR de l'UE et du Royaume-Uni, plusieurs lois des États-Unis (y compris la Loi californienne sur la protection de la vie privée des consommateurs) et les Principes australiens de protection de la vie privée de la Loi sur la protection de la vie privée de 1988 (Privacy Act 1988). Les informations personnelles comprennent les informations relatives à toute personne raisonnablement identifiable. Il peut s'agir, par exemple, de votre nom, âge, sexe, code postal et coordonnées.

Les informations sensibles comprennent les informations biométriques que nous traitons lorsque nous procédons à la comparaison des visages.

2. Avis spécial sur les données biométriques pour les résidents de l'Illinois, de Washington et du Texas

Pour les résidents de l'Illinois, de Washington ou du Texas, si nos clients vous demandent de leur fournir un document contenant votre photographie ou si vous devez vérifier ou authentifier votre identité en fournissant une photographie ou une vidéo de vous-même, les données dérivées de votre visage que nous collectons et traitons pour le compte de nos clients afin de fournir le service de vérification ou d'authentification peuvent être considérées

comme des données biométriques. Nous n'utiliserons vos données que dans le but de vérifier ou d'authentifier votre identité et de prévenir la fraude, et sans aucune autre fin. Vos données iométriques seront conservées aussi longtemps que nécessaire à ces fins, mais pas plus de trois ans.

3. Quelles sont les informations personnelles et sensibles que nous collectons et conservons?

Nous pouvons collecter et conserver les types d'informations personnelles et d'informations sensibles suivants:

- nom ;
- adresse postale ;
- numéro de téléphone portable ;
- adresse électronique ;
- âge ou date de naissance ;
- nationalité ;
- identifiants de types gouvernementaux, tels que le numéro et la catégorie de votre permis de conduire, votre numéro d'assurance maladie, le numéro de votre carte d'identité nationale ou fédérale, le numéro de votre passeport et le numéro de votre certificat de naissance ou de mariage ;
- indicateurs d'activité frauduleuse ;
- autres informations identifiables à partir des documents d'identité scannés que vous fournissez, comme votre statut de donneur d'organes ou les photographies de votre visage ;
- informations biométriques, telles que notre « Feature ID » (un hachage unidirectionnel) que nous créons à partir de séquences vidéo ou de photographies de votre visage ;
- informations obtenues par les services de prévention de la fraude et de vérification des documents ;
- identifiant de votre appareil, type d'appareil, informations de géolocalisation, informations relatives à l'ordinateur et à la connexion, adresse IP et informations standards du journal web ; et
- toute autre information personnelle qui peut être requise pour fournir nos services à nos clients.

4. Comment collectons nous vos informations personnelles et sensibles?

Nous pouvons collecter ces types d'informations personnelles ou sensibles soit directement auprès de vous, soit auprès de tiers lorsque vous utilisez nos services de vérification ou d'authentification.

Nous recevons et enregistrons automatiquement certaines informations provenant de votre appareil mobile. Il peut s'agir d'informations telles que le site Internet ou l'application tierce dans lequel les services sont intégrés, la date et l'heure auxquelles vous utilisez les services, votre adresse IP et votre nom de domaine, vos attributs logiciels et matériels (y compris le système d'exploitation, le modèle d'appareil et les informations d'empreinte digitale hachée de l'appareil) et votre situation géographique générale (par exemple, votre ville, votre état ou votre région métropolitaine).

Lorsque vous nous fournissez des informations personnelles ou sensibles au nom de quelqu'un d'autre, vous devez vous assurer que vous êtes autorisé à nous fournir ces informations personnelles ou sensibles. Vous devez également leur indiquer comment trouver une copie de cette Politique de protection de la vie privée.

Nous pouvons recevoir des informations personnelles, sensibles ou anonymes vous concernant de la part de nos clients lorsqu'ils font appel à nos services. Ces informations peuvent inclure un identifiant client qui vous identifie dans une base de données, ainsi que les catégories d'informations mentionnées ci-dessus.

Conservation de vos informations personnelles et sensibles

Nous conserverons vos informations personnelles et sensibles uniquement pendant la durée nécessaire aux fins énoncées dans la présente Politique de protection de la vie privée. Nous conserverons et utiliserons vos informations personnelles et sensibles dans la mesure nécessaire pour nous conformer à nos obligations légales (par exemple, si nous sommes tenus de conserver vos données pour nous conformer aux lois applicables), résoudre les litiges et appliquer nos politiques et accords juridiques.

5. Pourquoi collecter, conserver, utiliser et divulguer des informations personnelles et sensibles?

Nous pouvons collecter, conserver, utiliser et divulguer vos informations personnelles et sensibles aux fins suivantes:

- pour fournir des services de vérification ou d'authentification, lorsque vous cherchez à accéder à l'un des produits ou services de nos clients (ou aux produits ou services de tiers, lorsque nos clients agissent en tant que courtiers, revendeurs, référents ou représentants de ces parties);
- prévenir les comportements frauduleux sur nos produits pour l'un de nos clients ;

- pour exploiter, protéger, améliorer et optimiser notre site Internet ou nos applications, nos activités et l'expérience de nos clients et utilisateurs, par exemple pour effectuer des analyses, mener des recherches et créer de nouveaux produits. Nous utilisons des données synthétiques ou des informations sur les caractéristiques des documents (sans données personnelles) pour former nos algorithmes; et

- pour nous conformer à nos obligations légales, et pour éventuellement résoudre tout litige avec l'un de nos clients ou utilisateurs.

Nous pouvons également être autorisés à utiliser les informations personnelles à des fins liées aux objectifs susmentionnés.

Nous **n'utilisons pas** vos données personnelles ou biométriques pour former nos algorithmes ou nos produits.

Nous pouvons utiliser des informations dépersonnalisées et agrégées pour partager des informations sur les utilisateurs de nos services, par exemple en publiant un rapport sur les tendances de l'utilisation de ces services.

Si nous pensons que vous vous faites passer pour quelqu'un d'autre, que vous utilisez une fausse identité ou que vous utilisez une identité volée, nous pouvons conserver des identifiants uniques dans une base de données sur les fraudes pour nous permettre d'identifier si vous essayez à nouveau de commettre une fraude à notre encontre ou vis à vis de nos clients. Nous vérifions manuellement chaque entrée dans notre base de données sur les fraudes afin de nous assurer qu'aucune victime de fraude n'y figure. Veuillez contacter dpo@lexisnexisrisk.com si vous pensez que votre identifiant figure dans notre base de données sur les fraudes, sans raison valable.

6. Autres circonstances dans lesquelles nous pouvons être amenés à divulguer vos informations personnelles ou sensibles

Transactions commerciales

Si nous sommes impliqués dans une fusion, une acquisition ou une vente d'actifs, vos informations personnelles et sensibles peuvent être transférées. Nous nous efforcerons de vous avertir avant que vos informations personnelles et sensibles ne soient transférées et soumises à une autre Politique de protection de la vie privée.

Application de la loi

Dans certaines circonstances, nous pouvons être tenus de divulguer vos informations personnelles et sensibles si la loi l'exige ou en réponse à des demandes valables des autorités publiques (par exemple, un tribunal ou une agence gouvernementale).

Autres exigences légales

Nous pouvons divulguer vos informations personnelles et sensibles si nous pensons, en toute bonne foi, qu'une telle action est nécessaire pour:

- se conformer à une obligation légale;
- protéger et défendre les droits ou la propriété de la Société ;
- prévenir ou enquêter sur d'éventuels actes répréhensibles en rapport
- avec nos services ;
- protéger la sécurité personnelle des utilisateurs des services ou du public ; et
- se prémunir contre toute responsabilité juridique.

7. Utilisons-nous vos données personnelles à des fins de marketing direct?

Nous n'utilisons pas les informations personnelles qui nous sont fournies ou qui sont collectées dans le cadre de nos services de vérification d'identité ou d'authentification à des fins de marketing.

8. À qui divulguons-nous vos informations personnelles ?

Nous pouvons divulguer des informations personnelles (mais pas de données sensibles ou biométriques) aux fins décrites dans la présente Politique de protection de la vie privée:

- sociétés du groupe IDVerse lorsque cela est nécessaire pour fournir nos services à nos clients ;
- nos clients et des tiers (lorsque nos clients agissent en tant que revendeurs ou représentants de ces parties), lorsque vous cherchez à accéder à leurs produits et/ou services et qu'il leur est demandé de vérifier votre identité pour ce faire. Nous ne vendons aucune de vos données à des tiers ;
- nos employés et sous-traitants, aux fins de la gestion de nos produits et systèmes et de la fourniture de nos services ;
- fournisseurs et prestataires de services tiers (y compris les fournisseurs de services de vérification de documents pour nous aider à vérifier la validité des documents d'identité que vous nous communiquez, et d'autres fournisseurs pour l'exploitation de nos sites Internet et/ou de nos activités ou dans le cadre de la fourniture de nos produits et services) ;
- tiers spécifiques que vous avez autorisés à recevoir les informations que nous détenons ;

- autres personnes, y compris des agences gouvernementales, des organismes de réglementation et des organismes chargés de l'application de la loi, ou si la loi l'exige, l'autorise ou le permet ; et

- si la loi l'exige ou le permet.

9. Transfert à l'étranger d'informations personnelles et sensibles

Nous utilisons des instances localisées d'hébergement sur le cloud afin de limiter les transferts à l'étranger.

- Clients européens, britanniques et du Moyen-Orient – toutes les données sont traitées au sein de l'UE ou du Royaume-Uni.

- Amériques – toutes les données sont traitées aux États-Unis

- Asie-Pacifique – toutes les données sont traitées en Australie ou à Singapour

Nous pouvons procéder à des transferts limités de données à caractère personnel au sein des sociétés de notre groupe vers l'Australie ou les États-Unis, depuis le Royaume-Uni ou l'UE, afin de fournir à nos clients des services d'assistance et de suivi de la clientèle. Nous effectuons ce transfert conformément aux Clauses contractuelles types approuvées par l'UE (avec l'addendum britannique).

Pour vous envoyer un message SMS afin de lancer le processus de vérification, votre numéro de téléphone portable n'est traité qu'aux États-Unis (sauf pour les résidents australiens pour lesquels nous faisons appel à un fournisseur australien). Notre fournisseur SMS (Twilio Inc) exporte les données conformément à ses Règles commerciales contractuelles approuvées par la Commission européenne. Pour vérifier que votre adresse est au bon format, nous l'envoyons à un fournisseur unique, situé au Royaume -Uni, aux États-Unis ou en Australie. Nos fournisseurs exportent tous les données conformément aux Clauses contractuelles types approuvées par l'UE (avec l'addendum britannique). Ces fournisseurs sont certifiés ISO 27001 et SOC2.

10. Sécurité et stockage

Nous prenons la sécurité des données très au sérieux et faisons l'objet d'un audit externe selon les normes ISO 27001 et SOC2 Type 2, chaque année. Nous prenons toutes les mesures physiques, électroniques et procedurals possibles pour protéger vos informations personnelles et sensibles contre la perte ou l'accès, l'utilisation, l'interférence, la modification ou la suppression non autorisés. Les données des utilisateurs sont hébergées par AWS dans des environnements en cloud, gérés et contrôlés par nous-mêmes.

Entre autres, nous cryptons les informations personnelles et sensibles en transit et au repos et mettons en œuvre de solides procédures de reprise après sinistre et de continuité des activités.

Les informations personnelles et sensibles sont conservées dans un environnement sécurisé. Nous avons mis en place des mesures de sécurité destinées à protéger les informations personnelles et sensibles. Les principales méthodes de sécurisation du stockage des informations personnelles et sensibles sont les suivantes:

- Accès sécurisé aux dossiers électroniques et physiques contenant des informations personnelles et sensibles, grâce à des autorisations d'accès aux systèmes protégées par un mot de passe et à un accès sécurisé aux dossiers et espaces de stockage ;
- Accès réservé aux employés et sous-traitants autorisés d'OCR Labs qui ont besoin d'un accès pour effectuer leurs tâches quotidiennes ; et
- Différents niveaux d'accès en fonction du niveau d'autorité et du type d'informations personnelles et sensibles auxquelles il est nécessaire d'accéder.

Contrôles relatifs sur la façon dont les informations personnelles et sensibles sont extraites de l'environnement sécurisé et sur la manière dont elles sont utilisées et distribuées. Nous effectuons également régulièrement des audits de sécurité, des analyses de vulnérabilité et des tests de pénétration afin de garantir le respect des meilleures pratiques et des normes de sécurité.

11. Informations personnelles et sensibles non sollicitées

Il peut arriver qu'une personne nous fournisse des informations personnelles ou sensibles concernant une autre personne. Lorsque nous recevons des informations personnelles non sollicitées dont nous n'avons pas besoin aux fins décrites ci-dessus, nous détruisons ou dépersonnalisons ces informations dès que possible (si cela est licite et raisonnable de le faire).

12. Accès et correction de vos informations

Vous pouvez accéder aux informations personnelles que nous détenons à votre sujet en nous contactant à l'aide des coordonnées ci-dessous.

Il se peut que nous ne soyons pas en mesure de vous donner accès à toutes vos informations personnelles et, dans ce cas, nous vous fournirons un avis écrit en expliquant la raison. Nous pouvons également avoir besoin de verifier votre identité lors de la sollicitude de vos informations personnelles.

Il est également possible que nous n'ayons pas stocké vos informations personnelles lorsque nous les avons collectées pour effectuer des services de vérification et pour la réalisation des services.

Si vous pensez que les informations personnelles que nous détenons à votre sujet sont inexactes, périmées, incorrectes ou incomplètes, veuillez nous contacter rapidement pour que nous puissions prendre les mesures nécessaires et veiller à ce qu'elles soient corrigées.

13. Règlement général sur la protection des données (RGPD) et vie privée

Fondement juridique du traitement des données à caractère personnel en vertu du RGPD

Lorsque nous fournissons nos services à nos clients, nous agissons en tant que sous-traitant de nos clients (qui sont les responsables du traitement). Il appartient à nos clients d'établir la base juridique du traitement, mais cela sera fait sous l'une des conditions suivantes:

- Consentement : vous avez donné votre consentement au traitement des données biométriques à des fins d'identification ou d'authentification. C'est le seul motif pour lequel nous traiterons vos informations biométriques.
- Exécution d'un contrat : le traitement des données à caractère personnel est nécessaire à l'exécution d'un contrat entre vous et nos clients.
- Intérêts légitimes : le traitement de vos données à caractère personnel est nécessaire aux fins des intérêts légitimes poursuivis par notre client, sans vous porter indûment préjudice.

Vos droits

Nous nous engageons à respecter la confidentialité de vos données personnelles et à vous garantir l'exercice de vos droits.

Vous avez le droit, en vertu de la présente Politique de protection de la vie privée et de la loi en vigueur dans votre juridiction, de:

- **Demander l'accès à vos données personnelles.** Le droit d'accéder, de mettre à jour ou de supprimer les informations que nous détenons sur vous.
- **Demander la correction des données personnelles que nous détenons à votre sujet.** Vous avez le droit de faire corriger toute information incomplète ou inexacte que nous détenons à votre sujet. Nous offrons aux personnes passant le processus de vérification la possibilité de modifier les données saisies de manière incorrecte dans le cadre du processus de vérification d'identité.
- **Vous opposer au traitement de vos données personnelles.** Ce droit existe lorsque notre client s'appuie sur un intérêt légitime comme base juridique de son traitement et qu'un élément de votre situation particulière vous incite à vous opposer au traitement de vos données à caractère personnel pour cette même raison.
- **Demander la suppression de vos données personnelles.** Vous avez le droit de demander à nos clients de supprimer ou de retirer les données à caractère personnel que nous détenons lorsqu'il n'y a pas de raison valable pour que nous continuions à les traiter.
- **Demander le transfert de vos données personnelles.** Nous donnons à nos clients la possibilité d'exporter leurs données personnelles dans un format structuré, couramment

utilisé et lisible par machine. Vous pouvez leur demander une copie des données vous concernant que nous détenons en leur nom.

- **Retirer votre consentement.** Vous avez le droit de retirer votre consentement à l'utilisation de vos données biométriques. Si vous retirez votre consentement, il se peut que nous ne soyons plus en mesure de vous donner accès à certaines fonctionnalités spécifiques du service.

Exercice de vos droits en matière de protection des données

Vous pouvez exercer vos droits d'accès, de rectification, d'annulation et d'opposition en nous contactant. Veuillez noter que nous pouvons vous demander de vérifier votre identité avant de répondre à ces demandes. Si vous nous en faites la demande, nous ferons de notre mieux pour vous répondre dans les plus brefs délais. Si notre client est le responsable du traitement des données, nous lui transmettons la demande.

Vous disposez d'un droit de réclamation, auprès d'une autorité de protection des données, sur la collecte et l'utilisation de vos données personnelles. Pour plus d'informations, si vous vous trouvez dans l'Espace économique européen (EEE) ou au Royaume-Uni, veuillez contacter votre autorité locale de protection des données au sein de l'EEE ou au Royaume-Uni.

14. Utilisation de notre site Internet et des cookies

Lorsque vous visitez notre site Internet (mais pas lorsque vous utilisez nos services de vérification), nous pouvons utiliser des cookies.

Que sont les cookies? Les cookies sont de petits fichiers qui sont stockés sur votre ordinateur ou autre dispositif par votre navigateur Internet.

Un cookie nous permet de savoir si vous avez déjà utilisé nos services et peut stocker les préférences de l'utilisateur et d'autres informations.

Comment les cookies sont-ils utilisés? Les cookies peuvent par exemple être utilisés pour collecter des informations sur votre utilisation de nos services pendant la session en cours et au fil du temps, sur le système d'exploitation et le type de navigateur de votre ordinateur ou autre dispositif, sur votre fournisseur d'accès à Internet, sur votre nom de domaine et votre adresse IP, ainsi que sur votre situation géographique générale.

Comment éviter les cookies? Si vous êtes soucieux par la présence de cookies sur votre ordinateur ou votre dispositif, vous pouvez configurer votre navigateur de manière à ce qu'il refuse tous les cookies ou qu'il vous indique lorsqu'un cookie est en cours d'installation, ce qui vous permet de décider de l'accepter ou non.

Vous pouvez également supprimer les cookies de votre ordinateur.

Toutefois, si vous choisissez de bloquer ou de supprimer les cookies, certaines fonctionnalités de nos services peuvent ne pas fonctionner correctement.

15. Liens

Notre site Internet ou nos apps peuvent contenir des liens vers des sites Internet exploités par des tiers. Ces liens sont fournis pour des raisons de commodité et peuvent ne pas être à jour ou ne pas être maintenus.

Sauf indication contraire expresse, nous ne sommes pas responsables des pratiques en matière de respect de la vie privée de ces sites Internet liés, ni de leur contenu, et nous n'exerçons aucun contrôle sur ces sites Internet liés et n'avons aucun droit sur ces derniers.

Les politiques de protection de la vie privée qui s'appliquent à ces autres sites Internet peuvent différer sensiblement de notre Politique de protection de la vie privée, et nous encourageons donc les personnes à les lire avant d'utiliser ces sites Internet.

16. Déposer une réclamation

Si vous pensez que nous avons enfreint les règles de confidentialité et/ou les lois applicables en matière de protection des données, ou si vous souhaitez déposer une réclamation concernant la manière dont nous avons traité vos informations personnelles, vous pouvez nous contacter à l'adresse suivante : dpo@lexisnexisrisk.com.

Veuillez indiquer votre nom et décrire clairement votre réclamation. Nous accuserons réception de votre réclamation et vous répondrons au plus
vite.

Si vous estimez que nous n'avons pas résolu la réclamation de manière satisfaisante, nous vous fournirons des informations sur les autres mesures possibles, dont l'une consiste à déposer une plainte auprès de votre autorité locale de régulation en matière de protection de la vie privée.

17. Nous contacter

Pour plus d'informations sur notre Politique ou nos pratiques en matière de protection de la vie privée, pour accéder à vos informations personnelles ou les corriger, ou pour déposer une réclamation, veuillez nous contacter rapidement en utilisant les coordonnées indiquées ci-dessous:

Responsable de la Protection de la vie privée
E-mail : dpo@lexisnexisrisk.com

Adresse: Data Protection Officer, LexisNexis Risk Solutions, Global Reach, Dunleavy Drive, Cardiff CF11 0SN, UK

18. IDVerse, intégré au groupe OCR Labs

La présente Politique de protection de la vie privée couvre les entités suivantes, qui font partie du groupe OCR Labs:

- OCR Labs Pty Ltd (NSW, Australie)
- OCR Labs Global Ltd (société anglaise)
- OCR Labs Global (USA) Inc (société du Delaware)

19. Contacts commerciaux

Si vous êtes l'un de nos clients ou prospects, nous pouvons collecter plusieurs informations auprès de vous dans le cadre normal d'une vente (y compris votre nom, vos coordonnées et votre sexe).

Si nous avons collecté vos informations personnelles parce que vous êtes un représentant de l'un de nos partenaires ou clients actuels ou potentiels, nous pouvons vous envoyer des ommunications de marketing direct et des informations sur les services et produits offerts par les membres d'OCR Labs.

Cela peut prendre la forme de courriels, SMS, courrier ou autres formes de communication, conformément à la Loi sur la protection de la vie privée. Vous pouvez refuser de recevoir des documents de marketing de notre part en nous contactant aux coordonnées indiquées ci-dessous ou en utilisant les moyens de désinscription fournis (par exemple, un lien de désinscription). Si nous utilisons vos informations personnelles à des fins de marketing direct, nous veillerons à respecter nos obligations légales.

Pour les personnes travaillant pour nos clients ou nos clients potentiels, vos données personnelles sont traitées dans la juridiction où vous travaillez et peuvent également être transférées aux États-Unis par notre partenaire
Salesforce.

Nous traitons ces données pour le motif légitime de : Intérêts légitimes – le traitement de vos données à caractère personnel est nécessaire aux fins de nos intérêts légitimes, sans vous porter indûment préjudice. Veuillez contacter notre Responsable de la Protection de la vie privée (dpo@lexisnexisrisk.com) si vous souhaitez faire valoir l'un de vos droits en vertu de la loi nous étant applicable en tant que responsable du traitement des
données.

Version 6.3

Date d'entrée en vigueur: Avril 2025

La présente Politique de protection de la vie privée est revue et mise à jour au moins une fois par an.