IDVerse - Política Global de Privacidade

Esta Política de Privacidade explica como tratamos os dados de pessoas que utilizam nossos serviços de verificação ou autenticação. Há seções específicas ao final desta Política que tratam de como processamos dados de candidatos a vagas de emprego e de contatos comerciais.

1. Introdução

A privacidade é um direito humano fundamental. Suas informações pessoais são exatamente isso: suas. Na IDVerse, queremos que continuem assim. Por essa razão, a privacidade é primordial para nós em tudo o que fazemos, e estamos comprometidos em respeitar a sua privacidade.

Nossa Política de Privacidade estabelece como coletamos, mantemos, utilizamos, armazenamos e divulgamos seus dados pessoais e dados pessoais sensíveis. Podemos alterar esta Política de Privacidade periodicamente, mediante publicação das alterações em nosso website. Recomendamos que você consulte nosso website periodicamente para garantir que esteja ciente da versão vigente desta Política de Privacidade.

Para os fins desta Política de Privacidade, “nós”, “nos” ou “nosso(s)” refere-se às diferentes empresas da IDVerse, listadas ao final desta Política. Estamos sujeitos a diferentes legislações globais de proteção de dados, a depender do local em que você reside, incluindo o GDPR da União Europeia e do Reino Unido, diversas leis estaduais dos Estados Unidos, incluindo a California Consumer Privacy Act, e os Australian Privacy Principles previstos no Privacy Act 1988.

Dados pessoais incluem informações relativas a uma pessoa natural razoavelmente identificável. Por exemplo, podem incluir seu nome, idade, gênero, código postal e dados de contato.

Dados pessoais sensíveis incluem dados biométricos que tratamos quando realizamos a correspondência facial.

2. Aviso Especial sobre Dados Biométricos para Residentes de Illinois, Washington e Texas

Para residentes de Illinois, Washington ou Texas, caso nossos clientes exijam que você nos forneça qualquer documento que contenha sua fotografia, ou caso você precise verificar ou autenticar sua identidade mediante o fornecimento de uma fotografia ou vídeo de si mesmo, os dados derivados de sua face que coletamos e tratamos em nome de nossos clientes para a prestação do serviço de verificação ou autenticação poderão ser considerados dados biométricos.

Utilizaremos seus dados apenas para a finalidade de verificar ou autenticar sua identidade e para prevenção a fraudes, e para nenhuma outra finalidade. Não transferimos seus dados biométricos a

terceiros. Seus dados biométricos serão armazenados pelo período necessário para essas finalidades, mas nunca por prazo superior a três anos.

3. Quais dados pessoais e dados pessoais sensíveis coletamos e mantemos?

Podemos coletar e manter os seguintes tipos de dados pessoais e dados pessoais sensíveis:

- nome;
- endereço postal ou residencial;
- número de telefone celular;
- endereço de e-mail;
- idade ou data de nascimento;
- nacionalidade;
- identificadores emitidos por autoridades governamentais, tais como número e categoria de carteira de habilitação, número do Medicare, número de documento de identidade estadual ou nacional, número de passaporte e número de certidão de nascimento ou casamento;
- indicadores de atividade fraudulenta;
- outras informações identificáveis constantes de documentos digitalizados que você forneça, tais como condição de doador de órgãos, informações de saúde ou outros dados sensíveis constantes do documento;
- dados biométricos, tais como nosso “Feature ID” (um hash unidirecional) que criamos a partir de imagens de vídeo ou fotografias de sua face;
- informações obtidas de serviços de prevenção a fraudes e serviços de verificação documental;
- identificador do dispositivo, tipo de dispositivo, informações de geolocalização, informações do computador e da conexão, endereço IP e informações padrão de logs da web; e
- quaisquer outros dados pessoais que possam ser necessários para a prestação de nossos serviços aos nossos clientes.

4. Como coletamos seus dados pessoais e dados pessoais sensíveis?

Podemos coletar esses tipos de dados pessoais ou dados pessoais sensíveis diretamente de você ou de terceiros, quando você utiliza nossos serviços de verificação ou autenticação.

Recebemos e registramos automaticamente determinadas informações de seu dispositivo móvel. Isso pode incluir informações como o website ou aplicativo de terceiro no qual os serviços estão integrados, a data e hora em que você utiliza os serviços, seu endereço IP e nome de domínio, atributos de software e hardware (incluindo sistema operacional, modelo do dispositivo e informações de impressão digital

do dispositivo em formato hash), bem como sua localização geográfica geral (por exemplo, sua cidade, estado ou região metropolitana).

Quando você nos fornece dados pessoais ou dados pessoais sensíveis em nome de outra pessoa, você deve assegurar que está autorizado a nos fornecer tais dados pessoais ou dados pessoais sensíveis. Você também deverá informá-la sobre como acessar uma cópia desta Política de Privacidade.

Podemos receber dados pessoais, dados pessoais sensíveis ou dados anonimizados a seu respeito de nossos clientes quando eles utilizam nossos serviços. Essas informações podem incluir um identificador de cliente que o identifique em uma base de dados, bem como as categorias de informações indicadas acima.

Retenção de seus dados pessoais e dados pessoais sensíveis

Reteremos seus dados pessoais e dados pessoais sensíveis apenas pelo período necessário para as finalidades estabelecidas nesta Política de Privacidade. Reteremos e utilizaremos seus dados pessoais e dados pessoais sensíveis na medida necessária para cumprir nossas obrigações legais, por exemplo, caso sejamos obrigados a reter seus dados para cumprir leis aplicáveis, resolver disputas e fazer cumprir nossos instrumentos jurídicos e políticas.

5. Por que coletamos, mantemos, utilizamos e divulgamos dados pessoais e dados pessoais sensíveis?

Utilizamos seus dados pessoais em nome de nossos clientes. A única exceção ocorre quando prestamos serviços no âmbito do UK Digital Identity and Attribute Trust Framework; nesse caso, consulte a Seção 14 abaixo.

Finalidade

Podemos coletar, manter, utilizar e divulgar seus dados pessoais e dados pessoais sensíveis para as seguintes finalidades:

- prestar serviços de verificação ou autenticação quando você busca acessar um dos produtos ou serviços de nossos clientes (ou produtos ou serviços de terceiros, quando nossos clientes atuam como corretores, revendedores, no âmbito de indicações ou representantes dessas partes);
- prevenir condutas fraudulentas praticadas em nossos produtos em relação a qualquer um de nossos clientes;
- operar, proteger, aprimorar e otimizar nosso website ou aplicativos, nosso negócio e a experiência de nossos clientes e usuários, inclusive para realizar análises, conduzir pesquisas e criar novos produtos. Utilizamos dados sintéticos ou informações sobre características de documentos, sem dados pessoais, para treinar nossos algoritmos; e

- cumprir nossas obrigações legais e, eventualmente, resolver quaisquer disputas que possamos ter com nossos clientes ou usuários.

Também podemos estar autorizados a utilizar dados pessoais para qualquer finalidade relacionada às finalidades acima.

Não utilizamos seus dados pessoais ou dados biométricos para treinar nossos algoritmos.

Não transferimos seus dados biométricos a qualquer outra parte, com exceção do cliente para o qual estamos verificando sua identidade.

Podemos utilizar informações desidentificadas e agregadas para compartilhar insights sobre usuários de nossos serviços, por exemplo, por meio da publicação de relatórios sobre tendências de uso desses serviços.

Como tratamos seus dados

Assim que coletamos seus dados, realizamos verificações totalmente automatizadas das evidências em nome de nossos clientes. Nossas verificações totalmente automatizadas podem incluir algumas ou todas as seguintes atividades:

- extração de dados dos documentos fornecidos por meio de tecnologia OCR;
- avaliação visual dos documentos fornecidos para identificar sinais de fraude, incluindo adulteração, fotocópia, deepfakes, substituição de fotografias, entre outros;
- verificação de que a selfie apresentada corresponde a uma pessoa real em um ambiente ao vivo. Podemos detectar quando são submetidas telas, fotografias, máscaras e deepfakes; e
- correspondência biométrica facial entre sua selfie e a imagem fotográfica constante dos documentos.

Retornamos ao nosso cliente as evidências coletadas e uma indicação sobre se nossa tecnologia detectou algum problema. Buscamos identificar sinais de fraude de identidade nas evidências que você nos fornece. Nosso cliente decidirá, então, quais serão os próximos passos. Nossos clientes configuram por quanto tempo armazenaremos seus dados pessoais, o que pode ser por período tão curto quanto uma semana, havendo um período máximo de três anos para dados biométricos.

Caso entendamos que você está se passando por outra pessoa, utilizando uma identidade sintética ou utilizando uma identidade furtada, poderemos reter identificadores únicos em uma base de dados antifraude para que possamos identificar eventual tentativa futura de fraude contra nós ou contra nossos clientes. Entre em contato pelo e-mail dpo@lexisnexisrisk.com caso entenda que seu identificador está em nossa base de dados antifraude e não deveria estar.

6. Outras circunstâncias em que podemos divulgar seus dados pessoais ou dados pessoais sensíveis

Operações societárias

Caso estejamos envolvidos em uma fusão, aquisição ou venda de ativos, seus dados pessoais e dados pessoais sensíveis poderão ser transferidos. Envidaremos esforços para fornecer aviso prévio antes que seus dados pessoais e dados pessoais sensíveis sejam transferidos e passem a estar sujeitos a uma Política de Privacidade diferente.

Autoridades públicas

Em determinadas circunstâncias, podemos ser obrigados a divulgar seus dados pessoais e dados pessoais sensíveis quando exigido por lei ou em resposta a solicitações válidas de autoridades públicas (por exemplo, um tribunal ou órgão governamental).

Outras exigências legais

Ocasionalmente, em determinadas circunstâncias limitadas, poderemos divulgar seus dados pessoais e dados pessoais sensíveis quando, de boa-fé, entendermos que tal medida é necessária para:

- cumprir uma obrigação legal;
- proteger e defender os direitos ou bens da Companhia;
- prevenir ou investigar possíveis irregularidades relacionadas aos nossos serviços;
- proteger a segurança pessoal dos usuários dos serviços ou do público; e
- proteger contra responsabilidade legal.

7. Utilizamos seus dados pessoais para marketing direto?

Não utilizamos dados pessoais fornecidos a nós ou coletados como parte de nossos serviços de verificação ou autenticação de identidade para fins de marketing.

Caso você seja um contato comercial, consulte a Seção 20 abaixo.

8. A quem divulgamos seus dados pessoais?

Podemos divulgar dados pessoais, mas não dados sensíveis ou biométricos, para as finalidades descritas nesta Política de Privacidade, às seguintes partes:

- empresas integrantes do grupo IDVerse, quando necessário para prestar nossos serviços aos nossos clientes;
- nossos clientes e terceiros (quando nossos clientes atuam como revendedores ou representantes desses terceiros), caso você esteja buscando acessar seus produtos e/ou serviços

e seja necessário verificar sua identidade para tanto. Não vendemos quaisquer de seus dados a terceiros;

- nossos empregados e contratados, para fins de gestão de nossos produtos e sistemas e prestação de nossos serviços;
- fornecedores e prestadores de serviços terceiros (incluindo prestadores de serviços de verificação documental para nos auxiliar a verificar a validade dos documentos de identidade que você nos disponibiliza, bem como outros fornecedores para a operação de nossos websites e/ou de nosso negócio ou em conexão com a prestação de nossos produtos e serviços a você);
- terceiros específicos autorizados por você a receber informações mantidas por nós;
- outras pessoas, incluindo órgãos governamentais, autoridades regulatórias e autoridades de aplicação da lei, ou conforme exigido, autorizado ou permitido por lei; e
- conforme de outra forma exigido ou permitido por lei.

9. Transferência internacional de dados pessoais e dados pessoais sensíveis

Utilizamos instâncias localizadas de hospedagem em nuvem para limitar transferências internacionais.

- Clientes da Europa, Reino Unido e Oriente Médio: todos os dados são tratados na União Europeia ou no Reino Unido.
- Américas: todos os dados são tratados nos Estados Unidos.
- Ásia-Pacífico: todos os dados são tratados na Austrália ou em Singapura.

Podemos realizar transferências limitadas de dados pessoais entre empresas do nosso grupo para a Austrália ou os Estados Unidos, a partir do Reino Unido ou da União Europeia, a fim de prestar serviços de suporte e customer success aos nossos clientes. As transferências são realizadas com base nas Cláusulas Contratuais Padrão aprovadas pela União Europeia, com o adendo do Reino Unido.

Para enviar uma mensagem SMS a você para iniciar a jornada de verificação, apenas seu número de telefone celular é tratado nos Estados Unidos (exceto no caso de residentes australianos, para os quais utilizamos um fornecedor australiano). Nosso provedor de SMS, Twilio Inc., exporta o número de telefone celular nos termos de suas Regras Corporativas Vinculantes aprovadas pela Comissão Europeia. Para verificar se seu endereço está no formato correto, enviamos apenas seu endereço a um fornecedor localizado no Reino Unido, nos Estados Unidos ou na Austrália. Todos os nossos fornecedores exportam o endereço com base nas Cláusulas Contratuais Padrão aprovadas pela União Europeia (com o adendo do Reino Unido). Esses fornecedores possuem certificações ISO 27001 e SOC 2.

10. Segurança e armazenamento

Levamos a segurança dos dados muito a sério e somos auditados externamente, todos os anos, em relação aos padrões ISO 27001 e SOC2 Tipo 2. Adotamos medidas físicas, eletrônicas e procedimentais

razoáveis para proteger seus dados pessoais e dados pessoais sensíveis contra perda ou acesso, uso, interferência, modificação ou exclusão não autorizados. Os dados dos usuários são hospedados pela AWS em ambientes de nuvem que gerenciamos e controlamos.

Entre outras medidas, criptografamos dados pessoais e dados pessoais sensíveis tanto em trânsito quanto em repouso e implementamos procedimentos robustos de recuperação de desastres e continuidade de negócios.

Os dados pessoais e dados pessoais sensíveis serão mantidos em ambiente seguro. Possuímos medidas de segurança destinadas a proteger esses dados. Os principais métodos de segurança aplicados ao armazenamento de dados pessoais e dados pessoais sensíveis incluem:

- acesso seguro a registros eletrônicos e físicos que contenham dados pessoais e dados pessoais sensíveis, por meio de permissões de acesso protegidas por senha aos sistemas e acesso fisicamente protegido a arquivos e locais de armazenamento;
- acesso restrito a empregados e contratados autorizados da OCR Labs que necessitem acessar tais dados para desempenhar suas atividades diárias; e
- níveis variados de acesso, conforme o nível de autoridade e o tipo de dado pessoal ou dado pessoal sensível a ser acessado.

Também possuímos controles relativos à forma como dados pessoais e dados pessoais sensíveis são extraídos do ambiente seguro e como são utilizados e distribuídos. Além disso, conduzimos regularmente auditorias de segurança, varreduras de vulnerabilidades e testes de penetração para assegurar conformidade com melhores práticas e padrões de segurança.

Não mantemos quaisquer dados de contato seus. No evento improvável de seus dados pessoais serem comprometidos enquanto estiverem sob nossa posse, informaremos o cliente em nome de quem mantemos seus dados, sendo provável que ele o informe de acordo com suas próprias obrigações de privacidade.

11. Dados pessoais e dados pessoais sensíveis não solicitados

Poderá haver circunstâncias em que uma pessoa nos forneça dados pessoais ou dados pessoais sensíveis de outra pessoa. Quando recebermos dados pessoais não solicitados que não sejam necessários para as finalidades descritas acima, destruiremos ou desidentificaremos tais informações assim que possível (desde que seja lícito e razoável fazê-lo).

12. Acesso e correção de suas informações

Você pode acessar os dados pessoais que mantemos sobre você entrando em contato conosco por meio das informações de contato abaixo.

Em alguns casos, talvez não possamos fornecer acesso a todos os seus dados pessoais e quando isso ocorrer, forneceremos a você uma notificação por escrito explicando o motivo. Também poderemos precisar verificar sua identidade quando você solicitar seus dados pessoais.

Ressaltamos que poderemos não ter armazenado seus dados pessoais quando eles tiverem sido coletados por nós para a prestação de serviços de verificação e tais serviços já tiverem sido concluídos.

Caso entenda que quaisquer dados pessoais que mantemos sobre você sejam inexatos, desatualizados, incorretos ou incompletos, entre em contato conosco prontamente, e adotaremos medidas razoáveis para assegurar sua correção.

13. Seus direitos

Base legal para o tratamento de dados pessoais sob o GDPR

Quando prestamos nossos serviços aos nossos clientes, atuamos como operadores em relação a nossos clientes, que são os controladores, ressalvada a exceção prevista na Seção 14 **abaixo**, na qual a IDVerse é, de fato, a controladora apenas no Reino Unido, no âmbito do Digital Identity and Attribute Trust Framework.

Cabe aos nossos clientes estabelecer a base legal para o tratamento, que será uma das seguintes:

- **Consentimento:** você forneceu seu consentimento para o tratamento de dados biométricos para fins de identificação ou autenticação, bem como para o tratamento automatizado de seus dados pessoais. Esta é a única base com fundamento na qual trataremos seus dados biométricos.
- **Execução de contrato:** o tratamento de dados pessoais é necessário para a execução de um contrato entre você e nossos clientes.
- **Interesses legítimos:** o tratamento de seus dados pessoais é necessário para atender aos interesses legítimos perseguidos por nosso cliente, desde que não o prejudique indevidamente.

Seus direitos

Comprometemo-nos a respeitar a confidencialidade de seus dados pessoais e a assegurar que você possa exercer seus direitos.

Nos termos desta Política de Privacidade e da legislação aplicável, conforme sua jurisdição, você tem o direito de:

- **Solicitar acesso aos seus dados pessoais.** Direito de acessar, atualizar ou excluir as informações que mantemos sobre você.

- **Solicitar a correção dos dados pessoais que mantemos sobre você.** Você tem o direito de solicitar a correção de qualquer informação incompleta ou inexata que mantemos sobre você. Oferecemos às pessoas que estamos verificando a oportunidade de alterar dados capturados incorretamente como parte da jornada de verificação de identidade.
- **Opor-se ao tratamento de seus dados pessoais.** Esse direito existe quando nosso cliente se baseia em interesse legítimo como fundamento legal para o tratamento e há algo em sua situação particular que o leve a se opor ao tratamento de seus dados pessoais com base nesse fundamento.
- **Solicitar a exclusão de seus dados pessoais.** Você tem o direito de solicitar aos nossos clientes que excluam ou removam dados pessoais que mantemos quando não houver motivo legítimo para continuarmos a tratá-los.
- **Solicitar a transferência de seus dados pessoais.** Disponibilizamos aos nossos clientes a possibilidade de exportar seus dados pessoais em formato estruturado, comumente utilizado e legível por máquina. Você pode solicitar a eles uma cópia dos dados que mantemos sobre você em nome deles.
- **Decisões automatizadas.** O serviço que prestamos é totalmente automatizado ao fornecer aos nossos clientes uma indicação do risco de fraude, e nossos clientes utilizarão nossos resultados como parte de sua decisão geral sobre sua identidade. Você deverá entrar em contato com nosso cliente caso queira solicitar informações sobre como ele utiliza os resultados de nossas verificações antifraude.
- **Retirar seu consentimento.** Você tem o direito de retirar seu consentimento para o uso de seus dados. Caso retire seu consentimento, talvez não possamos fornecer acesso a determinadas funcionalidades específicas do serviço.

Exercício de seus direitos de proteção de dados

Você poderá exercer seus direitos de acesso, retificação, cancelamento e oposição entrando em contato conosco. Observe que poderemos solicitar a verificação de sua identidade antes de responder a tais solicitações. Caso você apresente uma solicitação, envidaremos nossos melhores esforços para respondê-la o quanto antes. Quando nosso cliente for o controlador dos dados, encaminharemos a solicitação a ele.

Você tem o direito de apresentar reclamação a uma Autoridade de Proteção de Dados sobre a coleta e o uso de seus dados pessoais por nós. Para mais informações, caso você esteja no Espaço Econômico Europeu ou no Reino Unido, entre em contato com a autoridade local de proteção de dados do EEE ou do Reino Unido.

14. UK Digital Identity and Attribute Trust Framework — IDVerse como controladora

O serviço da IDVerse permite a verificação única da identidade de uma pessoa viva. Essa verificação é realizada de acordo com as regras estabelecidas no UK Digital Identity and Attributes Trust Framework, do Department for Science, Innovation and Technology do Reino Unido (o "**UKDIATF**").

A IDVerse é certificada no âmbito do UKDIATF para verificações de identidade para fins de DBS (Disclosure and Barring Service), Right to Work e Right to Rent. Você não precisa pagar à IDVerse por esse serviço, mas a IDVerse cobrará seus clientes.

No âmbito do UKDIATF, a IDVerse atua como controladora de seus dados pessoais, pois deve determinar como seus dados são tratados e deve decidir se você foi corretamente verificado de acordo com as regras do UKDIATF. Uma vez que a IDVerse transfere seus dados aos seus clientes, esses clientes passam a atuar, de forma independente, como controladores de seus dados.

Como a IDVerse trata seus dados de forma lícita no âmbito do UKDIATF

- **Consentimento:** para o tratamento de dados biométricos (sua face para correspondência facial e verificações de vivacidade) e para decisões automatizadas, você deverá fornecer consentimento explícito à IDVerse; e
- **Interesses legítimos:** para o tratamento de seus dados pessoais não biométricos, a IDVerse realiza o tratamento com base em seus interesses legítimos de prestar um serviço a seus clientes.

Compartilhamento de dados no âmbito do UKDIATF

Todos os dados coletados de você são compartilhados com nossos clientes. A Seção 3 acima lista os dados coletados.

A IDVerse utilizará fornecedores terceiros de dados para verificar indicadores de fraude e a exatidão dos dados fornecidos:

- **Synectics:** verificamos suas informações em relação às bases National SIRA e NFI. Você pode ler mais sobre a Synectics em: https://www.synectics-solutions.com/privacy-policy
- **Loqate, uma empresa do grupo GBG Group plc:** verificamos se o endereço fornecido atende à estrutura e ao formato esperados, enviando apenas seu endereço à Loqate.
- **Twilio:** enviamos apenas seu número de telefone celular à Twilio para que ela possa enviar um link por SMS ao seu celular.

Consulte as Seções 13 e 17 para informações sobre seus direitos e sobre como apresentar uma reclamação.

15. Uso de nosso website e cookies

Quando você visita nosso website, mas não quando utiliza nossos serviços de verificação, podemos instalar cookies.

O que são cookies? Cookies são pequenos arquivos armazenados em seu computador ou outro dispositivo por seu navegador.

Um cookie nos permite reconhecer se você já utilizou nossos serviços anteriormente e pode armazenar preferências do usuário e outras informações.

Como os cookies são utilizados? Por exemplo, cookies podem ser utilizados para coletar informações sobre o uso de nossos serviços durante sua sessão atual e ao longo do tempo, sobre o sistema operacional e tipo de navegador de seu computador ou outro dispositivo, seu provedor de serviços de internet, seu nome de domínio e endereço IP, bem como sua localização geográfica geral.

Como evitar cookies? Caso você esteja preocupado com a presença de cookies em seu computador ou dispositivo, pode configurar seu navegador para recusar todos os cookies ou para indicar quando um cookie estiver sendo instalado, permitindo que você decida se deseja aceitá-lo.

Você também pode excluir cookies de seu computador.

No entanto, se optar por bloquear ou excluir cookies, determinadas funcionalidades de nossos serviços poderão não funcionar corretamente.

16. Links

Nosso website ou aplicativos podem conter links para websites operados por terceiros. Esses links são fornecidos por conveniência e podem deixar de estar atualizados ou mantidos.

Salvo disposição expressa em contrário, não somos responsáveis pelas práticas de privacidade ou por qualquer conteúdo constante desses websites vinculados, e não temos controle sobre eles nem direitos sobre tais websites.

As políticas de privacidade aplicáveis a esses outros websites podem diferir substancialmente de nossa Política de Privacidade, razão pela qual recomendamos que os indivíduos as leiam antes de utilizar tais websites.

17. Apresentação de reclamação

Caso entenda que violamos leis de privacidade e/ou de proteção de dados aplicáveis, ou caso deseje apresentar uma reclamação sobre a forma como tratamos seus dados pessoais, você pode entrar em contato conosco pelo e-mail dpo@lexisnexisrisk.com.

Inclua seu nome e descreva claramente sua reclamação.

Acusaremos o recebimento de sua reclamação e responderemos dentro de prazo razoável.

Caso entenda que não resolvemos a reclamação de forma satisfatória, forneceremos informações sobre as etapas adicionais que você poderá adotar, incluindo a possibilidade de apresentar reclamação à autoridade local de privacidade.

18. Fale conosco

Para obter mais informações sobre nossa Política de Privacidade ou nossas práticas, acessar ou corrigir seus dados pessoais, ou apresentar uma reclamação, entre em contato conosco prontamente por meio dos dados abaixo:

Privacy Office
E-mail: dpo@lexisnexisrisk.com

Endereço:
Data Protection Officer
LexisNexis Risk Solutions
Global Reach, Dunleavy Drive
Cardiff CF11 0SN
Reino Unido

19. IDVerse, parte do OCR Labs Group

Esta Política de Privacidade abrange as seguintes entidades, que integram o OCR Labs Group:

- OCR Labs Pty Ltd (sociedade em NSW, Austrália);
- OCR Labs Global Ltd (sociedade inglesa); e
- OCR Labs Global (USA) Inc (sociedade em Delaware).

20. Contatos comerciais

Caso você seja nosso cliente ou potencial cliente, podemos coletar determinadas informações suas no curso normal de uma venda a você (incluindo seu nome, dados de contato e cargo).

Caso tenhamos coletado seus dados pessoais porque você é representante de um de nossos parceiros ou clientes atuais ou potenciais, podemos enviar a você comunicações de marketing direto e informações sobre serviços e produtos oferecidos por membros da OCR Labs. Isso pode ocorrer por e-mail, SMS, correio ou outras formas de comunicação, em conformidade com o Privacy Act. Você pode optar por não receber materiais de marketing entrando em contato conosco por meio dos dados indicados abaixo ou utilizando os mecanismos de descadastramento disponibilizados (por exemplo, um

link de cancelamento de inscrição). Caso utilizemos seus dados pessoais para marketing direto, asseguraremos o cumprimento de nossas obrigações legais.

Para indivíduos que trabalham para nossos clientes ou potenciais clientes, seus dados pessoais são tratados na jurisdição em que você atua e também podem ser transferidos para os Estados Unidos por nosso parceiro Salesforce.

Caso você trabalhe em uma empresa que seja potencial cliente nossa, podemos transferir seus dados de contato a parceiros comerciais ou a uma empresa do grupo para que essa entidade entre em contato com você sobre o uso da IDVerse.

Tratamos esses dados com fundamento na seguinte base legal: **legítimo interesse** – o tratamento de seus dados pessoais é necessário para atender aos interesses legítimos perseguidos por nós, desde que não prejudique você indevidamente.

Entre em contato com nosso Privacy Officer pelo e-mail dpo@lexisnexisrisk.com caso deseje exercer quaisquer de seus direitos nos termos da legislação aplicável a nós como controladores de dados.

Serviços Credenciados de Identidade Digital (Austrália)

Para serviços prestados nos termos do Digital ID Act 2024:

- dados biométricos não são retidos após a verificação, exceto quando permitido pela Lei para prevenção a fraudes e segurança do sistema;
- qualquer retenção dessa natureza é limitada, controlada e automaticamente excluída dentro de prazos definidos; e
- os controles de tratamento de dados são fixos e não configuráveis pelos clientes.

Versão 6.5

Data de vigência: maio de 2026

Esta Política de Privacidade é revisada e atualizada, no mínimo, anualmente.