Global Privacy Policy

プライバシーは基本的人権です。 あなたの個人情報はまさにあなたのものです。 OCR Labs では、それを維持したいと考えています。 そのため、当社はあらゆる活動においてプライバシーを最優先しており、お客様のプライバシーを尊重することに努めています。

当社のプライバシー ポリシーは、当社がお客様の個人情報および機密情報を収集、保持、使用、保管、開示する方法を定めています。 当社は、プライバシー ポリシーへの変更を当社 Web サイトに公開することにより、随時変更する場合があります。 当社の現在のプライバシー ポリシーを確実に認識するために、当社の Web サイトを定期的にチェックすることをお勧めします。

このプライバシー ポリシーの目的上、「当社」とは、OCR Lab のさまざまな事業 (本ポリシーの最後に記載) を意味します。 当社は、EU および英国の GDPR、CCPA、および 1988 年プライバシー法におけるオーストラリアのプライバシー原則を含む世界的なデータ保護法に拘束され、基礎となる州および準州の同等の法律の遵守を保証します。

個人情報には、合理的に特定可能な個人に関する情報または意見 (真実かどうかにかかわらず) が含まれます。 たとえば、これにはあなたの名前、年齢、性別、郵便番号、連絡先の詳細が含まれる場合があります。

機密情報には、顔照合を実行するときに処理する生体認証情報が含まれます。 このプライバシー ポリシーは、当社の現従業員および元従業員の従業員記録に関連する行為および慣行には適用されません。

イリノイ州、ワシントン州、テキサス州の居住者に対する特別な生体認証データに関する通知

イリノイ、ワシントン、またはテキサスにお住まいの場合、お客様がお客様の写真を含む文書の提供を当社に要求した場合、またはお客様がご自身の写真やビデオを提供して身元を確認または認証する必要がある場合、お客様の顔から抽出されたデータ 検証または認証サービスを提供するために当社がクライアントに代わって収集および処理するデータは、一部の管轄区域では生体認証データとみなされる場合があります。 当社は、お客様のデータを本人確認または認証および詐欺防止の目的でのみ使用し、その他の目的では使用しません。 お客様のデータは、これらの目的に必要な限り保管されますが、3 年を超えないものとします。

1. 私たちはどのような個人情報や機密情報を収集し、保持していますか?

当社は、次の種類の個人情報および機密情報を収集および保持する場合があります。

- 名前
- 郵送先または住所

LexisNexis® RISK SOLUTIONS

- 電子メールアドレス
- 電話番号
- 年齢または生年月日
- 国籍
- 政府関連の識別子（免許証番号および等級、メディケア番号、州または国民 ID カード番号、パスポート番号、出生証明書または結婚証明書の番号など）
- 不正行為の兆候
- 臓器提供者のステータスや顔写真など、お客様が提供したスキャンされた身分証明書から特定できるその他の情報
- ビデオ映像や顔の写真から当社が作成したテンプレートなどの生体認証情報
- 不正行為防止サービスおよび文書検証サービスから取得した情報
- デバイス ID、デバイス タイプ、地理的位置情報、コンピュータと接続情報、IP アドレス、および標準の Web ログ情報
- 当社の Web サイトやアプリを通じて直接、または当社の Web サイトやアプリの使用やオンライン プレゼンスを通じて間接的に、あるいは当社が情報収集を許可した他の Web サイトやアカウントを通じて、お客様が当社に提供したお客様に関する追加情報
- クライアントまたは顧客アンケートを通じてお客様が当社に提供する情報
- 当社との取引を促進するために必要となるその他の個人情報

2. あなたの個人情報や機密情報はどのように収集されますか?

当社は、これらの種類の個人情報または機密情報をお客様から直接、または第三者から収集する場合があります。 当社は次の場合にこの情報を収集することがあります。

- 当社のアプリまたはウェブベースのプラットフォームのいずれかを介して、当社の検証または認証サービスのいずれかを利用する。
- あなたが当社のパートナーまたはクライアントの代表者である場合、管理者アカウントを作成するか、当社のパートナーまたはクライアントのいずれかに代わって当社のアプリまたはウェブベースのプラットフォームのいずれかを使用します。
- 通信、チャット、電子メール、または当社の Web サイトを通じて当社と通信する。 または

- それ以外の場合は、当社のサイト、サービス、コンテンツ、または広告とやり取りします。

お客様が当社の検証サービスまたは認証サービスをご利用になると、当社はお客様のコンピュータ (またはその他のデバイス) および/または Web ブラウザから特定の情報を自動的に受信し、記録します。

これには、サービスが統合されているサードパーティの Web サイトまたはアプリケーション、サービスを使用した日時、IP アドレスとドメイン名、ソフトウェアとハードウェアの属性 (オペレーティング システム、デバイス モデル、ハッシュ化されたデバイスの指紋情報）、および一般的な地理的位置（都市、州、大都市圏など）が含まれます。

このような情報を取得するために、当社はお客様のコンピュータを認識し、そのオンライン活動に関する情報を収集するウェブログまたはアプリケーションを使用する場合があります。

他人に代わって個人情報または機密情報を当社に提供する場合、その個人情報または機密情報を当社に提供することが許可されていることを確認する必要があります。 また、このプライバシー ポリシーのコピーを見つける方法も伝える必要があります。

当社は、当社のサービスを利用するクライアントから、お客様に関する個人情報、機密情報、または匿名化された情報を受け取る場合があります。 この情報には、サードパーティのデータベース内でお客様を識別するクライアント ID や、上記のカテゴリの情報が含まれる場合があります。 当社は、お客様以外の別の情報源から個人情報や機密情報を収集する場所について、できるだけ早くお知らせします。

個人情報や機密情報の保持

当社は、このプライバシー ポリシーに定められた目的に必要な期間のみ、お客様の個人情報および機密情報を保持します。 当社は、法的義務を遵守し（たとえば、適用法を遵守するためにお客様のデータを保持する必要がある場合）、紛争を解決し、当社の法的契約とポリシーを施行するために必要な範囲で、お客様の個人情報および機密情報を保持および使用します。

3. なぜ個人情報や機密情報を収集、保持、使用、開示するのでしょうか?

当社が個人情報および機密情報を使用する目的は、お客様との関係およびお客様が当社に要求する製品またはサービスによって異なります。 当社は、以下の目的でお客様の個人情報および機密情報を収集、保持、使用および開示する場合があります。

- お客様が当社の Web サイトまたはアプリにアクセスして使用できるようにするため。
- 当社の顧客の製品またはサービスのいずれか (または、当社の顧客が仲介者、再販業者、紹介者または代理人として機能する場合には、第三者の製品またはサービス) にアクセスしようとする場合に、検証または認証サービスを提供するため。

- 当社の顧客に対して当社の製品に対して行われる不正行為を防止するため。
- 分析の実行、調査の実施、新製品の作成など、当社の Web サイトやアプリ、ビジネス、クライアントおよびユーザーのエクスペリエンスを運用、保護、改善、最適化するため。 当社は、アルゴリズムをトレーニングするために、合成データまたは文書の特性に関する情報 (個人データは含まない) を使用します。 アルゴリズムのトレーニングにお客様の個人データや生体認証データを使用することはありません。
- サービス、サポートおよび管理メッセージ、リマインダー、技術通知、アップデート、当社の検証サービスに関連するセキュリティ警告、およびお客様が要求した情報を送信するため。
- 当社の法的義務を遵守し、当社のクライアントまたはユーザーとの間で生じる可能性のある紛争を解決し、第三者との契約を強制するため。
- 必要に応じて、雇用への応募を検討するため。

私たちには次の権利も与えられる場合があります。

- 上記の目的に関連する目的で個人情報を使用する。
- 上記の目的に直接関連する目的で機密情報を使用すること。

また、当社は、検証サービスの使用傾向に関するレポートを発行するなどして、検証サービスのユーザーに関する洞察を共有するために、匿名化された集約情報を使用する場合もあります。 お客様が誰かになりすましていたり、合成 ID を使用したり、盗んだ ID を使用したりしていると当社が判断した場合、お客様が当社または当社のクライアントに対して再び詐欺を行おうとした場合に識別できるように、当社は一意の ID を不正データベースに保持する場合があります。 当社では、不正データベースの各エントリを手動でチェックし、不正の被害者がデータベースに登録されていないことを確認します。 あなたの識別子が当社の不正データベースに含まれるべきではないと思われる場合は、dpo@lexisnexisrisk.com までご連絡ください。

4. 当社がお客様の個人情報または機密情報を開示する可能性があるその他の状況

商取引

当社が合併、買収、資産売却に関与した場合、お客様の個人情報や機密情報が転送される可能性があります。 当社は、お客様の個人情報や機密情報が転送され、別のプライバシー ポリシーの適用を受ける前に通知するよう努めます。

法執行機関

特定の状況下では、法律で要求された場合、または公的機関 (裁判所や政府機関など) からの有効な要求に応じて、お客様の個人情報や機密情報の開示を求められる場合があります。

その他の法的要件

当社は、その措置が必要であると判断される際、以下の目的でお客様の個人情報や機密情報を開示する場合があります。

- 法的義務を遵守するため。
    - 会社の権利または財産を保護および弁護するため。
    - 当社のサービスに関連して起こり得る不正行為を防止または調査するため。
    - サービスのユーザーまたは公衆の個人の安全を保護するため。
    - 法的責任から保護するため。

5. ダイレクトマーケティングのためにあなたの個人情報を使用しますか?

あなたが当社の現在または将来のパートナーまたはクライアントの代表者であるために当社が個人情報を収集した場合、当社は、OCR Labs のメンバーが提供するサービスおよび製品に関するダイレクトマーケティングコミュニケーションおよび情報を送信することがあります。

これは、プライバシー法に従って、電子メール、SMS、郵便、またはその他の通信形式をとる場合があります。

後段に記載の詳細を使用して当社に連絡するか、提供されるオプトアウト機能 (購読解除リンクなど) を使用することにより、当社からのマーケティング資料の受信をオプトアウトできます。

当社がダイレクト マーケティングにお客様の個人情報を使用する場合、オーストラリアの 2006 年電話登録禁止法および 2003 年スパム法に基づく義務を確実に遵守します。

当社は、本人確認サービスの一環として収集した個人情報をマーケティング目的で使用することはありません。

6. あなたの個人情報は誰に開示されますか?

当社は、このプライバシー ポリシーに記載されている目的で、個人情報 (ただし、機密データや生体認証データは除く) を次の目的で開示する場合があります。

- OCR Labs グループ内の企業。
    - 当社の顧客および第三者 (当社の顧客が再販業者またはその代理人として機能する場合)。お客様がその製品および/またはサービスにアクセスしようとしており、そのために本人確認を要求される場合。 当社はお客様のデータを第三者に販売することはありません。

- 当社の製品およびシステムを管理し、当社のサービスを提供する目的のための当社の従業員および請負業者。
- 第三者のサプライヤーおよびサービスプロバイダー (お客様が当社に開示する身分証明書の有効性を当社が検証するのに役立つ文書検証サービスのプロバイダー、および当社の Web サイトまたは当社の事業の運営のため、あるいは当社の製品およびサービスの提供に関連するその他のプロバイダーを含みます) 。
- 専門のアドバイザー、ディーラー、代理店。
- 当社の既存または潜在的な代理店、ビジネスパートナーまたはパートナー (当社の信頼できる再販業者および紹介者を含む)。
- 当社が保有する情報を受け取ることをお客様が許可した特定の第三者。
- 政府機関、規制機関、法執行機関を含むその他の人物、または法律で要求、認可、許可されている場合。 そして
- 法律で別途要求または許可されている場合。

7. 個人情報および機密情報の海外移転

当社の本人確認サービスをご利用される個人の方

海外への転送を制限するために、クラウド ホスティングのローカライズされたインスタンスを使用します。

- ヨーロッパ、英国、中東のクライアント – すべてのデータは EU または英国内で処理されます。
- アメリカ – すべてのデータは米国内で処理されます。
- アジア太平洋 – すべてのデータはオーストラリア国内で処理されます。

クライアントの連絡先

当社の顧客または将来の顧客のために働く個人の場合、個人データは事業を展開する管轄区域内で処理され、当社のパートナーである Salesforce によって米国に転送される場合もあります。

8. セキュリティとストレージ

当社はデータ セキュリティを非常に重視しており、ISO 27001 および SOC2 Type 2 標準に基づいて外部監査を毎年受けています。 当社は、お客様の個人情報および機密情報を紛失または不正なアクセス、使用、妨害、変更、または削除から保護するために、合理的な物理的、電子的、

および手続き上の措置を講じます。 ユーザーデータは、AWS が管理および制御するクラウド環境でホストされます。

何よりも、当社は転送中および保存中の個人情報および機密情報を暗号化し、堅牢な災害復旧および事業継続手順を実装しています。

個人情報や機密情報は安全な環境で保管されます。 当社では、個人情報や機密情報を保護することを目的としたセキュリティ対策を講じています。 個人情報や機密情報を安全に保管する主な方法には次のようなものがあります。

- パスワードで保護されたシステムへのアクセス許可、およびファイル キャビネットやストレージへのセキュリティで保護されたアクセスを通じて、個人情報や機密情報を含む電子的および物理的記録への安全なアクセス。
    - 日々の業務を遂行するためにアクセスを必要とする、認可された OCR Labs の従業員および請負業者のみがアクセスできます。 そして
    - 権限のレベルと、アクセスが必要な個人情報および機密情報の種類に応じて、アクセス レベルが変化します。

個人情報や機密情報を安全な環境から抽出する方法、およびその使用方法と配布方法に関する制御。 また、セキュリティ監査、脆弱性スキャン、侵入テストを定期的に実施し、セキュリティのベスト プラクティスと標準への準拠を保証します。

9. 未承諾の個人情報および機密情報

状況によっては、個人が他の人の個人情報または機密情報を当社に提供する場合があります。当社が上記の目的に必要のない一方的な個人情報を受け取った場合、当社は可能な限り速やかにその情報を破棄または匿名化します（そうすることが合法的かつ合理的である場合）。

10. 自分の情報へのアクセスと修正

以下の連絡先情報を使用して当社にご連絡いただくことで、当社が保持するお客様の個人情報にアクセスできます。

場合によっては、当社はお客様のすべての個人情報へのアクセスを提供できない場合があります。その場合は、その理由を説明した書面による通知をお客様に提供します。 また、お客様が個人情報を要求する場合、当社はお客様の身元を確認する必要がある場合もあります。

当社は、検証サービスを実行するために当社がお客様の個人情報を収集し、そのようなサービスが完了した場所にはお客様の個人情報を保管していない可能性があることに注意してください。

当社が保持するお客様の個人情報が不正確、古い、間違っている、または不完全であると思われる場合は、速やかに当社にご連絡ください。確実に修正するために合理的な措置を講じます。

11. 一般データ保護規則 (GDPR) のプライバシー

GDPR に基づく個人データ処理の法的根拠

当社は以下の条件下で個人データを処理する場合があります。

- 同意: 1 つ以上の特定の目的で機密データや個人データを処理することに同意したことになります。
    - 契約の履行: 個人データの提供は、お客様との契約の履行および契約前の義務のために必要です。
    - 法的義務: 個人データの処理は、当社が従うべき法的義務を遵守するために必要です。
    - 正当な利益: 個人データの処理は、お客様に不当に害を及ぼさない当社が追求する正当な利益の目的のために必要です。
    - いずれの場合でも、当社は、処理に適用される具体的な法的根拠、特に個人データの提供が法定要件なのか契約要件なのか、それとも契約締結に必要な要件なのかを明確にするために喜んで協力します。

あなたの権利

当社は、お客様の個人データの機密性を尊重し、お客様が権利を行使できることを保証することを約束します。

あなたは、このプライバシー ポリシーに基づき、また管轄区域に応じて法律により、次の権利を有します。

- **自分の個人データへのアクセス要求。** 当社がお客様に関して保有する情報にアクセス、更新、または削除する権利。 可能な場合はいつでも、アカウント設定セクション内で直接、個人データにアクセス、更新、または削除をリクエストできます。 これらの操作をご自身で実行できない場合は、弊社までご連絡ください。 これにより、当社が保持するお客様の個人データのコピーを受け取ることもできます。
- **当社が保持するお客様の個人データの修正要求。** あなたには、当社が保持するあなたに関する不完全または不正確な情報を修正してもらう権利があります。 当社は、本人確認作業の一環として、認証対象の個人に、誤って取得されたデータを修正する機会を提供します。

- **個人データ処理への異議申し立て。** この権利は、当社が当社の処理の法的根拠として正当な利益に依存しており、お客様の特定の状況に関して何らかの事情があり、この理由に基づいて当社によるお客様の個人データの処理に反対したい場合に存在します。 また、お客様には、当社がダイレクト マーケティング目的でお客様の個人データを処理する場合に異議を申し立てる権利もあります。

- **個人データ消去の要求。** 当社が個人データの処理を継続する正当な理由がない場合、お客様は当社に個人データの削除または削除を要求する権利を有します。

- **個人データの転送要求。** 当社は、構造化された一般的に使用される機械可読形式で、お客様またはお客様が選択した第三者にお客様の個人データを提供します。 この権利は、お客様が最初に当社の使用に同意した自動情報、または当社がお客様との契約を履行するためにその情報を使用した自動情報にのみ適用されることにご注意ください。

- **同意の撤回。** あなたには、自分の個人データの使用に関する同意を撤回する権利があります。 同意を撤回すると、サービスの特定の機能へのアクセスを提供できなくなる場合があります。 これを行うには、dpo@lexisnexisrisk.com に電子メールを送信してください。

データ保護の権利の行使

お客様は、当社にご連絡いただくことで、アクセス、修正、キャンセル、異議申し立ての権利を行使することができます。 かかるリクエストに応答する前に、お客様の身元確認をお願いする場合があることにご注意ください。 ご要望がございましたら、できるだけ早く対応させていただきます。

お客様には、当社によるお客様の個人データの収集および使用についてデータ保護当局に苦情を申し立てる権利があります。 詳細については、欧州経済領域 (EEA) または英国にお住まいの場合は、EEA または英国の地域のデータ保護当局にお問い合わせください。

12. 当社のウェブサイトとクッキーの使用

お客様が当社の Web サイトにアクセスすると (当社の検証サービスを使用する場合は除きます)、Cookie がドロップされる場合があります。

Cookieとは何ですか? Cookie は、Web ブラウザによってコンピュータまたはその他のデバイスに保存される小さなファイルです。 Cookie を使用すると、お客様が以前に当社のサービスを使用したかどうかを認識し、ユーザーの好みやその他の情報を保存することができます。

Cookieはどのように使用されますか? たとえば、Cookie は、現在のセッションおよび中長期にわたる当社のサービスの使用状況、コンピュータまたはその他のデバイスのオペレーティング システムとブラウザの種類、インターネット サービス プロバイダー、ドメイン名と IP アドレス、および一般的な位置情報を収集するために使用できます。

Cookieを避けるにはどうすればよいですか? コンピューターまたはデバイスに Cookie が存在することに懸念がある場合は、すべての Cookie を拒否するようにブラウザを設定するか、Cookie が設定されるタイミングを示すようにブラウザを設定して、Cookie を受け入れるかどうかを決定できます。

コンピューターから Cookie を削除することもできます。

ただし、Cookie をブロックまたは削除することを選択した場合、当社のサービスの特定の機能が正しく動作しなくなる可能性があります。

13. リンク

当社のウェブサイトまたはアプリには、第三者が運営するウェブサイトへのリンクが含まれている場合があります。 これらのリンクは便宜のために提供されており、最新のものではない可能性があります。

14. 苦情の申し立て

当社がプライバシー法および/または適用されるデータ保護法に違反したと思われる場合、または当社によるお客様の個人情報の取り扱い方法について苦情を申し立てたい場合は、以下に記載の詳細を使用して当社にご連絡ください。

お名前、電子メールアドレス、電話番号を記入し、苦情を明確に説明してください。

当社はお客様の苦情を認識し、合理的な期間内にお客様の苦情に関して回答します。

当社が苦情を十分に解決できなかったと思われる場合は、お客様が講じることができるさらなる手順に関する情報を提供します。その 1 つは、オーストラリア情報コミッショナー局に苦情を申し立てることです。

15. お問い合わせ

当社のプライバシー ポリシーや慣行に関する詳細情報、またはお客様の個人情報へのアクセスまたは修正、苦情の申し立てについては、以下に記載の詳細を使用して速やかにご連絡ください。

プライバシー責任者 : dpo@lexisnexisrisk.com 郵送先: Data Protection Officer, LexisNexis Risk Solutions, Global Reach, Dunleavy Drive, Cardiff CF11 0SN, UK

16. OCR Labs Group

このプライバシー ポリシーは、OCR Labs グループの一部を構成する次の組織を対象としています。

- OCR Labs Pty Ltd (オーストラリア、ニューサウスウェールズ州の会社)

- OCR Labs Global Ltd（英国の会社）
- OCR Labs Global (USA) Inc (デラウェア州の会社)

発効日: 2025 年4月

＜Original in English ＞

Privacy is a fundamental human right. Your personal information is exactly that, yours. At OCR Labs, we want to keep it that way. That is why privacy is paramount to us, in everything we do, and we are committed to respecting your privacy.

Our Privacy Policy sets out how we collect, hold, use, store and disclose your personal and sensitive information. We may change our Privacy Policy from time to time by publishing changes to it on our website. We encourage you to check our website periodically to ensure that you are aware of our current Privacy Policy.

For the purposes of this Privacy Policy, ‘us’ ‘we’ or ‘our’ means the OCR Lab’s different businesses (listed at the end of this Policy). We are bound by global data protection legislation including the EU and UK GDPR, CCPA and the Australian Privacy Principles in the Privacy Act 1988 and ensure compliance with underlying state and territories equivalent legislation.

Personal information includes information or an opinion (whether true or not) about an individual that is reasonably identifiable. For example, this may include your name, age, gender, postcode and contact details.

Sensitive information includes biometric information we process when we perform face matching. This Privacy Policy does not apply to acts and practices in relation to employee records of our current and former employees.

Special Biometric Data Notice for Illinois, Washington and Texas Residents

For residents of Illinois, Washington or Texas, if our clients require you to provide us with any document that contains your photograph or if you need to verify or authenticate your identity by providing a photograph or video of yourself, the data derived from your face that we collect and process on behalf of our clients to provide the verification or authentication service may be considered biometric data in some jurisdictions. We will only use your data for the purpose of verifying or authenticating your identity and the prevention of fraud, and for no other purpose. Your data will be stored as long as required for these purposes, but no longer than three years.

1. What personal and sensitive information do we collect and hold?

We may collect and hold the following types of personal information and sensitive information:

- name;

- mailing or street address;
- email address;
- telephone number;
- age or date of birth;
- nationality;
- government related identifiers, such as your licence number and class, Medicare number, state or national ID card number, passport number, and birth or marriage certificate number;
- indicators of fraudulent activity;
- other information identifiable from scanned ID documents you provide, such as your organ donor status or photographs of your face;
- biometric information, such as templates we create from video footage or photographs of your face;
- information obtained from fraud-prevention services and document verification services;
- your device ID, device type, geo-location information, computer and connection information, IP address and standard web log information;
- any additional information relating to you that you provide to us directly through our website or apps or indirectly through your use of our website or apps or online presence or through other websites or accounts from which you permit us to collect information;
- information you provide to us through client or customer surveys; and
- any other personal information that may be required in order to facilitate your dealings with us.

2. How do we collect your personal and sensitive information?

We may collect these types of personal or sensitive information either directly from you, or from third parties. We may collect this information when you:

- utilise one of our verification or authentication services through one of our apps or web-based platforms;

- if you are a representative of one of our partners or clients, create an administrator account or otherwise use one of our apps or web-based platforms on behalf of one of our partners or clients;
- communicate with us through correspondence, chats, email or otherwise through our website; or
- otherwise interact with our sites, services, content or advertising.

When you use our verification or authentication services, we automatically receive and record certain information from your computer (or other device) and/or your web browser.

This may include such information as the third-party website or application into which the services are integrated, the date and time that you use the services, your IP address and domain name, your software and hardware attributes (including operating system, device model, and hashed device fingerprint information), and your general geographic location (e.g., your city, state, or metropolitan region).

To obtain such information, we may use web logs or applications that recognize your computer and gather information about its online activity.

Where you provide us with personal or sensitive information on behalf of someone else, you must ensure you are permitted to provide us with their personal or sensitive information. You also need to tell them how to find a copy of this Privacy Policy.

We may receive personal, sensitive or anonymised information about you from our clients where they make use of our services. This information may include a client ID that identifies you in the third party's database, as well as the categories of information set out above. We will advise you as soon as possible where we collect personal and sensitive information from another source other than yourself.

Retention of your personal and sensitive information

We will retain your personal and sensitive information only for as long as is necessary for the purposes set out in this Privacy Policy. We will retain and use your personal and sensitive information to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

3. Why do we collect, hold, use and disclose personal and sensitive information?

The purposes for which we will use personal and sensitive information will depend on the relationship with you and the products or services you require from us. We may collect, hold, use and disclose your personal and sensitive information for the following purposes:

- to enable you to access and use our website or apps;
- to provide verification or authentication services, where you are seeking to access one of our clients' products or services (or the products or services of third parties, where our clients act as brokers, resellers, referrers or representatives of such parties);
- to prevent fraudulent behaviour being undertaken on our products for any of our clients;
- to operate, protect, improve and optimise our website or apps, business and our clients' and users' experience, such as to perform analytics, conduct research and create new products. We use synthetic data or information about the characteristics of documents (with no personal data) to train our algorithms. We do not use your personal data or biometric data to train the algorithms;
- to send you service, support and administrative messages, reminders, technical notices, updates, security alerts in connection with our verification services, and information requested by you;
- to comply with our legal obligations, resolve any disputes that we may have with any of our clients or users, and enforce our agreements with third parties; and
- where relevant, to consider your employment application.

We may also be entitled:

- to use personal information for any purpose which is related to the above purposes; and
- to use sensitive information for any purpose which is directly related to the above purposes.

We may also use de-identified, aggregated information to share insights about users of our verification services, such as by publishing a report on trends in the usage of such services. If we think you are impersonating someone, using a synthetic identity or using a stolen identity then we may retain unique identifiers in a fraud database to allow us to identify if you try to commit fraud against us or our clients again. We check each entry into our fraud database manually to ensure no victims of fraud are put into it. Please contact dpo@lexisnexisrisk.com if you think your identifier is in our fraud database and should not be.

4. Other circumstances where we may disclosure of your personal or sensitive information

Business Transactions

If we are involved in a merger, acquisition or asset sale, your personal and sensitive information may be transferred. We will endeavour to provide notice before your personal and sensitive information is transferred and becomes subject to a different Privacy Policy.

Law enforcement

Under certain circumstances, we may be required to disclose your personal and sensitive information if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

Other legal requirements

We may disclose your personal and sensitive information in the good faith belief that such action is necessary to:

- comply with a legal obligation;
- protect and defend the rights or property of the Company;
- prevent or investigate possible wrongdoing in connection with our services;
- protect the personal safety of users of the services or the public;
- protect against legal liability.

5. Do we use your personal information for direct marketing?

If we have collected your personal information because you are a representative of one of our current or prospective partners or clients, we may send you direct marketing communications and information about services and products offered by members of OCR Labs.

This may take the form of emails, SMS, mail or other forms of communication, in accordance with the Privacy Act.

You may opt-out of receiving marketing materials from us by contacting us using the details set out below or by using the opt-out facilities provided (e.g. an unsubscribe link).

If we use your personal information for direct marketing, we will ensure we comply with our obligations under the *Australian Do Not Call Register Act 2006* and the *Spam Act 2003*.

We do not use personal information collected as part of our identity verification services for marketing purposes.

6. To whom do we disclose your personal information?

We may disclose personal information (but not sensitive or biometric data) for the purposes described in this Privacy Policy to:

- companies within the OCR Labs group;

- our clients and third parties (where our clients act as resellers or representatives of such parties), where you are seeking to access their products and/or services and are required to verify your identity in order to do so. We do not sell any of your data to any third party;
- our employees and contractors, for the purposes of managing our products and systems and providing our services;
- third party suppliers and service providers (including providers of document verification services to help us verify the validity of identity documents you disclose to us, and other providers for the operation of our websites and/or our business or in connection with providing our products and services to you);
- professional advisers, dealers and agents;
- our existing or potential agents, business partners or partners (including our trusted resellers and referrers);
- specific third parties authorised by you to receive information held by us;
- other persons, including government agencies, regulatory bodies and law enforcement agencies, or as required, authorised or permitted by law; and
- as otherwise required or permitted by law.

7. Overseas transfer of personal and sensitive information

Individuals using our identity verification services

We use localised instances of cloud hosting so that overseas transfers are limited.

- European, UK and Middle Eastern clients – all data is processed within the EU or the UK
- Americas – all data is processed within the USA
- Asia-Pacific – all data is processed within Australia

Client contacts

For individuals working for our clients or prospective clients your personal data is processed within the jurisdiction you operate in and may also be transferred to the USA by our partner Salesforce.

8. Security and storage

We take data security very seriously and are externally audited against the ISO 27001 and SOC2 Type 2 standards each year. We take reasonable physical, electronic, and procedural measures to protect your personal and sensitive information against loss or unauthorised access, use,

interference, modification, or deletion. User data is hosted by AWS in cloud environments which we manage and control.

Among other things, we encrypt personal and sensitive information both in transit and at rest and we implement robust disaster recovery and business continuity procedures.

Personal and sensitive information will be held in a secure environment. We have security measures in place which are intended to protect personal and sensitive information. The key methods of securing the storage of personal and sensitive information include:

- Secure access to electronic and physical records containing personal and sensitive information, via password protected access permissions to systems and security-protected access to filing cabinets and storage;
- Access only to authorised OCR Labs employees and contractors that require access to perform their daily duties; and
- Varying access levels depending on the level of the authority and the type of personal and sensitive information required to be accessed.

Controls relating to how personal and sensitive information is extracted from the secure environment and how it is used and distributed. We also regularly conduct security audits, vulnerability scans, and penetration tests to ensure compliance with security best practices and standards.

9. Unsolicited personal and sensitive information

There may be circumstances where an individual provides us with the personal or sensitive information about another person. Where we receive unsolicited personal information which we do not require for the purposes we have outlined above, we will destroy or de-identity that information as soon as practicable (if it is lawful and reasonable to do so).

10. Accessing and correcting your information

You can access the personal information we hold about you by contacting us using the contact information below.

Sometimes, we may not be able to provide you with access to all of your personal information and, where this is the case, we will provide you with a written notice explaining why. We may also need to verify your identity when you request your personal information.

We note that we may not have stored your personal information where it was collected by us to perform verification services and such services have been completed.

If you think that any personal information we hold about you is inaccurate, outdated, incorrect or incomplete, please contact us promptly and we will take reasonable steps to ensure that it is corrected.

11. General Data Protection Regulation (GDPR) Privacy

Legal Basis for Processing Personal Data under GDPR

We may process personal data under the following conditions:

- Consent: you have given your consent for processing sensitive and personal data for one or more specific purposes.
- Performance of a contract: provision of personal data is necessary for the performance of an agreement with you and/or for any pre-contractual obligations thereof.
- Legal obligations: processing personal data is necessary for compliance with a legal obligation to which we are subject to.
- Legitimate interests: processing personal data is necessary for the purposes of the legitimate interests pursued by us which does not unduly prejudice you.
- In any case, we will gladly help to clarify the specific legal basis that applies to the processing, and in particular whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract.

Your Rights

We undertake to respect the confidentiality of your personal data and to guarantee you can exercise your rights.

You have the right under this Privacy Policy, and by law depending on your jurisdiction, to:

- **Request access to your personal data.** The right to access, update or delete the information we have on you. Whenever made possible, you can access, update or request deletion of your personal data directly within your account settings section. If you are unable to perform these actions yourself, please contact us to assist you. This also enables you to receive a copy of the personal data we hold about you.
- **Request correction of the personal data that we hold about you.** You have the right to have any incomplete or inaccurate information we hold about you corrected. We offer individuals we are verifying the opportunity to amend incorrectly captured data as part of the identity verification journey.

- **Object to processing of your personal data.** This right exists where we are relying on a legitimate interest as the legal basis for our processing and there is something about your particular situation, which makes you want to object to our processing of your personal data on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes.

- **Request erasure of your personal data.** You have the right to ask us to delete or remove personal data when there is no good reason for us to continue processing it.

- **Request the transfer of your personal data.** We will provide to you, or to a third-party you have chosen, your personal data in a structured, commonly used, machine-readable format. Please note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

- **Withdraw your consent.** You have the right to withdraw your consent on using your personal data. If you withdraw your consent, we may not be able to provide you with access to certain specific functionalities of the service. You can this by emailing dpo@lexisnexisrisk.com.

Exercising of Your Data Protection Rights

You may exercise your rights of access, rectification, cancellation and opposition by contacting us. Please note that we may ask you to verify your identity before responding to such requests. If you make a request, we will try our best to respond to you as soon as possible.

You have the right to complain to a Data Protection Authority about Our collection and use of your personal data. For more information, if you are in the European Economic Area (EEA) or the UK, please contact Your local data protection authority in the EEA or the UK.

12. Using our website and cookies

When you visit our website (but not when you use our verification services) we may drop cookies.

What are cookies? Cookies are small files that are stored on your computer or other device by your web browser. A cookie allows us to recognize whether you have used our services before and may store user preferences and other information.

How are cookies used? For example, cookies can be used to collect information about your use of our services during your current session and over time, your computer or other device's operating system and browser type, your Internet service provider, your domain name and IP address, and your general geographic location.

How do you avoid cookies? If you are concerned about having cookies on your computer or device, you can set your browser to refuse all cookies or to indicate when a cookie is being set, allowing you to decide whether to accept it.

You can also delete cookies from your computer.

However, if you choose to block or delete cookies, certain features of our services may not operate correctly.

13. Links

Our website or apps may contain links to websites operated by third parties. Those links are provided for convenience and may not remain current or be maintained.

Unless expressly stated otherwise, we are not responsible for the privacy practices of, or any content on, those linked websites, and have no control over or rights in those linked websites.

The privacy policies that apply to those other websites may differ substantially from our Privacy Policy, so we encourage individuals to read them before using those websites.

14. Making a complaint

If you think we have breached the Privacy and/or applicable data protection laws, or you wish to make a complaint about the way we have handled your personal information, you can contact us using the details set out below.

Please include your name, email address and/or telephone number and clearly describe your complaint.

We will acknowledge your complaint and respond to you regarding your complaint within a reasonable period of time.

If you think that we have failed to resolve the complaint satisfactorily, we will provide you with information about the further steps you can take, one of which is to lodge a complaint with the Office of the Australian Information Commissioner.

15. Contact us

For further information about our Privacy Policy or practices, or to access or correct your personal information, or make a complaint, please contact us promptly using the details set out below:

Privacy Office e: dpo@lexisnexisrisk.com a: Data Protection Officer, LexisNexis Risk Solutions, Global Reach, Dunleavy Drive, Cardiff CF11 0SN, UK

16. OCR Labs Group

This Privacy Policy covers the following entities, which form part of the OCR Labs Group:

- OCR Labs Pty Ltd (NSW, Australia company)
- OCR Labs Global Ltd (English company)
- OCR Labs Global (USA) Inc (Delaware company)

Effective Date: April 2025