Australian Privacy Policy

This Privacy Policy explains how we process the data of people who use our verification or authentication services. There are separate sections at the end of the policy covering how we process data of job applicants and business contacts.

1. Introduction

Privacy is a fundamental human right. Your personal information is exactly that, yours. At IDVerse a LexisNexis Risk Solutions Company, 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 OCR Labs Pty Limited (ABN 603 823 276). We are bound by the Australian Privacy Principles in the Privacy Act 1988 and ensure compliance with underlying state and territories equivalent legislation.

Personal information includes information 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.

2. 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;
- mobile 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 documents you provide, such as your organ donor status, health information or other sensitive data on the document;
- biometric information, such as our 'Feature ID' (a one way hash) 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; and
- any other personal information that may be required in order to provide our services to our clients.

3. 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 when you use our verification or authentication services.

We automatically receive and record certain information from your mobile device. 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).

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 a database, as well as the categories of information set out above.

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.

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

Purpose

We may collect, hold, use and disclose your personal and sensitive information for the following purposes:

- 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; and
- to comply with our legal obligations, and perhaps to resolve any disputes that we may have with any of our clients or users.

We may also be entitled to use personal information for any purpose which is related to the above purposes.

We do **not** use your personal data or biometric data to train our algorithms.

We do **not** transfer your biometric data to any other party (with the exception of the client for whom we are verifying your identity for).

We may use de-identified, aggregated information to share insights about users of our services, such as by publishing a report on trends in the usage of such services.

How we process your data

As soon as we have collected data from you we perform fully automated checks on the evidence on behalf of our clients. Our fully automated checks could include some or all of the following:

a. extraction of the data from the provided documents using OCR technology;

b. a visual assessment of the provided documents for signs of fraud; including tampering, photocopying, deepfakes, replacing photos etc;

c. ensuring that the selfie presented is of a real person in a live environment. We can detect when screens, photos, masks and deepfakes are submitted;

d. a biometric face match between your selfie and the photo image on the documents; and

e. if a client requests we may check your identity matches the records held by the government body that issued the original document.

We return to our client the evidence collected and an indication of whether our technology has detected any issues. We are looking for signs of identity fraud in the evidence you provide to us. Our client will then decide what its next steps will be.

Our clients configure how long we store your personal data for, which could be as short as one week, and there is a maximum period of three years for biometric data.

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. Please contact dpo@lexisnexisrisk.com if you think your identifier is in our fraud database and should not be.

5. 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

On occasion in certain limited circumstances 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; and

- protect against legal liability.

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

We do not use personal information provided to us or collected as part of our identity verification or authentication services for marketing purposes.

7. 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 IDVerse group where necessary to provide our services to our clients;
- 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;
- the document issuer to check your identity matches the records held on the DVS. Please see www.idmatch.gov.au for more information and you can email: dvs.manager@ag.gov.au;
- 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);
- 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.

8. Overseas transfer of personal and sensitive information

We use localised instances of cloud hosting so that overseas transfers are limited. For Australian and NZ residents interacting with Australian or NZ clients all data is processed within Australia

We may make limited transfers of personal data to our group companies in the USA or the UK in order to provide support and customer success services to our clients. Those group companies are subject to exactly the same technical and organisational security controls as our Australian company, and those group companies are audited annually by an external auditor.

To check that your address is in the right format we send your address only to a supplier in either the UK or the USA. Those suppliers are ISO 27001 and SOC2 certified.

9. 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 IDVerse 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.

10. 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).

11. 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.

12. 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.
- **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 our client is relying on a legitimate interest as the legal basis for its processing and there is something about your particular situation, which makes you want to object to its processing of your personal data on this ground.
- **Request erasure of your personal data.** You have the right to ask our clients to delete or remove personal data that we are holding when there is no good reason for us to continue processing it.
- **Request the transfer of your personal data.** We give the ability to export your personal data in a structured, commonly used, machine-readable format. You can ask them for a copy of the data we hold on their behalf about you.
- **Automated Decision Making.** The service we provide is fully automated in providing to our clients an indication of the risk of fraud, and our clients will use our results as part of their overall decision as to your identity. You will need to contact our client if you want to ask for information about how it uses the results of our fraud checks.

- **Withdraw your consent.** You have the right to withdraw your consent on using your data. If you withdraw your consent, we may not be able to provide you with access to certain specific functionalities of the service.

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. Where our client is the data controller we will pass on the request to them.

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.

13. 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.

14. 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.

15. 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 at dpo@lexisnexisrisk.com.

Please include your name 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.

16. 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 Officer

e: dpo@lexisnexisrisk.com

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

17. Privacy Impact Assessment (PIA) Register

REF.	DATE SIGNED	SHORT DESCRIPTION
PIA_v1.1	Oct-18	Initial draft covering core verification services (Orbit SDK)
PIA_v2.0	Jan-19	IDVaaS based upon Orbit SDK engines, including updates on the recommendations from PIA_v1.1
PIA_v3.0	Aug-21	Updated Privacy Impact Assessment

PIA_4.0	Feb-23	Updated Privacy Impact Assessment
PIA_5.0	Feb-24	Updated Privacy Impact Assessment

18. Privacy: Transparency Report

IDVerse is committed to being transparent about government requests for customer data and how we respond. We publish an annual Transparency Report disclosing the number of government requests for customer data IDVerse receives.

Government and private entities are required to follow applicable laws and statutes when requesting customer information and data from IDVerse.

Report: 1 July 2023 – 30 June 2024

No requests received.

19. Business contacts

If you are a client or prospect of ours then we may collect certain information from you in the ordinary course of a sale to you (including your name, contact details and title).

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.

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.

If you work at a prospective client of ours then we may transfer your contact details to a sales' partners for that entity to get in touch with you about using IDVerse.

Please contact our Privacy Officer (dpo@lexisnexisrisk.com) if you wish to enforce any of your rights under the applicable law that applies to us as data controller.

Version 6.4

Effective Date: April 2025

This Privacy Policy is review and updated at least annually.