Face Access™ Privacy Policy

This Privacy Policy only covers our Authentication product. If you are using our Identity Verification product then please refer to our Global Privacy Policy here.

For the purposes of this Privacy Policy, 'us' 'we' or 'our' means IDVerse'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.

Special Biometric Data Notice for Illinois, Washington and Texas Residents

For residents of Illinois, Washington or Texas, if our clients require you to 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 authentication service may be considered biometric data in some jurisdictions. We will only use your data for the purpose of 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 information do we process, how do we collect it and how long do we keep it?

To provide the authentication service we collect a selfie image from the liveness video that we ask you to complete. Our client will also provide us with another picture of you (either from their database or we will take it from the database we manage for them). We will create biometrics of each image and try and match them.

We collect and retain your consent confirmation (if provided directly to us).

We also collect information like IP address and device information to help with anti-fraud checks by us and our clients.

We retain the data for as long as a client requests us to. Biometric data is always deleted within three years at the very latest.

2. Why and how do we use your data?

Our clients are asking you to perform the authentication check so that they can be sure it is really you returning to use their services. We also collect the IP address and device information and pass to our client so that they can use for fraud checks.

We may also use de-identified, aggregated information to understand and share insights about users of our 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 onto 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.

3. 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 data 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.

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, or if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency);
- protect and defend our rights or property, protect against our legal liability;
- prevent or investigate possible wrongdoing in connection with our services; and
- protect the personal safety of users of the services or the public.

4. Overseas transfer

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

- European 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 or Singapore

5. Security and storage

We take data security very seriously and are externally audited against the ISO 27001 and SOC2 Type 2 standards each year. For more information please the Security and storage section in the Global Privacy Policy.

6. 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, deletion or correction of your personal data.** If you wish to access, delete or correct data we are holding on you then please contact the entity which asked you to use our services.

- **Withdraw your consent.** You have the right to withdraw your consent on using your personal data. If you withdraw your consent, our client may not be able to provide you with same service. You should contact the entity that asked you to use this service or by emailing dpo@lexisnexisrisk.com.

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.

7. Making a complaint

If you think we have breached applicable data protection laws, or you wish to make a complaint, you can contact us using the details set out below. Please include your name and email address and clearly describe your complaint.

We will acknowledge your complaint and respond to you 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 applicable privacy regulator.

8. 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:

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

9. IDVerse Group

IDVerse is a trading name of OCR Labs. 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)