

LexisNexis® IDU® App Privacy Notice

This Privacy Notice contains the following sections:

- What this Privacy Notice covers
- How we use personal data
- What personal data is collected and from whom it is obtained
- How personal data is shared and retained
- How you can request to access, correct, delete your personal data or ask us not to process your personal data
- How to contact us

What this Privacy Notice covers

This Privacy Notice applies to the processing of personal data through the LexisNexis® IDU® App (“App”). (“App”) and is provided by LexisNexis Risk Solutions Group (“**LNRS**”, “**we**” or “**us**”), part of the RELX Group™ of companies.

The App is used by our clients to carry out identification checks to help them check the identities of people applying for or receiving products or services; to assist them in complying with regulations such as anti-money laundering (AML), anti-bribery and corruption or other legal requirements; to help them to prevent and investigate fraud and other potential offences.

Our clients may also need to complete further identity checks for purposes such as the above as well as for the prevention and detection of fraud or other potential offences. This processing is done via our IDU® product and further details how your personal data is processed within IDU® can be found via - <https://risk.lexisnexis.co.uk/processing-notices/business>

Please see the ‘How we use your personal data’ section below, which will explain how LNRS will process your personal data via the App.

- ***Who controls your personal data***

LNRS are a data controller for the App and control the processing of the personal data obtained within it.

There may be cases where a client asks us to complete additional identification checks, where we process these on behalf of our clients we are data processors.

The clients who use our services are also data controllers. Their privacy notices will tell you more about how they use personal data.

How we use your personal data

We may process your personal information within the App for the purposes described in this Privacy Notice.

Before you choose to use the App to verify your identity, your service provider (our client) will provide you an alternative method to complete identity verification, if you are happy with the App method, LNRS will obtain your consent for processing any biometric data within the App. Please see the section below - Sensitive personal data/Special category personal data for further information on biometric data. We will only process your personal data within the App for the purposes of verifying your identity as described within this Privacy Notice.

- **Using personal data for our and our Customers' legitimate interests**

We use personal data in the App to perform identity verification services, this assists clients in checking the identities of people applying for or receiving products or services; in some cases this may be to assist them in their compliance with regulation, such as, anti-money laundering (AML), anti-bribery and corruption or other legal requirements. Additionally helping clients to prevent and investigate fraud and other potential offences. We may also use personal data to develop and improve our products and services

The exact information that is collected depends on the check the clients instructs us to perform. For example, when verifying an identity, we may ask for an image of you and your identity document(s), we make an automated assessment on whether the document is authentic and whether the pictured individual is likely to be the same person as the image. Clients may also check your name and address against addresses obtained from trusted public sources, like the Electoral Register.

When we carry out an identity check on behalf of our clients, we produce a report of the results for the client. In some cases, the report from a check will be 'yes' or 'no'; in other cases we may provide more detail. We provide our clients with this information in order to empower them to make informed decisions about individuals.

Our Customers are responsible for how they may use the results of a check performed using our products or services – for example, whether our Customer decides that they are permitted to do business with a particular client is solely up to them. The personal data we provide to them and which we describe below is one factor they may consider in that assessment.

What data is collected and from whom it is obtained

In order to begin the process of verifying your identity via the App we will receive your personal data from the Client for you to use the App.

Personal data collected will be dependent upon the Client requirements. For specific details regarding the personal data collected, please contact the Client.

Your photographic image will be provided directly by you to us via the App.

LNRS may process personal data including (but not limited to).

- your name
- your date of birth
- your address
- email address
- telephone number

- documentation such as passport or driving licence; and
- photographic image.

Sensitive personal data/Special category personal data

The App requires you to upload a document containing a photographic image e.g. passport or driving license and a ‘selfie’. A faceprint will be generated from the photographic image on your document and the ‘selfie’ to compare likeness. The faceprint is unique to an individual and is considered as biometric data and therefore a special category of personal data under the European General Data Protection Regulation (“EU GDPR”) and United Kingdom General Data Protection Regulation (“UK GDPR”). In order for us to process your photographic image, LNRS requires your consent. LNRS captures this consent within the App before the images are requested.

How personal data is shared and retained

- ***With whom we share personal data and how we safeguard transfers of personal data***

We share personal data with the categories of third parties described below. Where personal data transferred to a country outside the UK or European Economic Area ("EEA"), we safeguard the data as described below.

Category	Description
<p>Service providers and data partners</p>	<p>We share personal data with service providers who assist us with the provision of our products and services. These providers include customer support, IT service providers, and professional advisors.</p> <p>Your personal information may be stored and processed in your region or another country where LexisNexis Risk Solutions Group affiliates and our service providers maintain servers and facilities, including but not limited to, Germany, Israel, the United Kingdom, and the United States. We take steps, including through contracts, intended to ensure that the information continues to be protected wherever it is located in a manner consistent with the standards of protection required under applicable law.</p>
<p>Other affiliated companies of LexisNexis® Risk Solutions Group within the RELX Group of companies</p>	<p>Some of the service providers we use are other affiliated companies of LNRS within the RELX group of companies. These companies assist us in providing the products and services described in this Notice, such as to provide customer and product support. We have contracts in place with them to ensure they only use the personal data we provide them in accordance with our instructions. Some of our affiliated companies also act as resellers, distributors, integrators or agents for the sale of LNRS products or services.</p>

	<p>Your personal information may be stored and processed in your region or another country where LexisNexis Risk Solutions Group affiliates and our service providers maintain servers and facilities, including but not limited to, Germany, Israel, the United Kingdom, and the United States. We take steps, including through contracts, intended to ensure that the information continues to be protected wherever it is located in a manner consistent with the standards of protection required under applicable law.</p> <p>Certain U.S. entities within the LexisNexis Risk Solutions group of companies have certified certain of their services to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks as set forth by the U.S. Department of Commerce. Please view these entities' Privacy Shield Notices here. To learn more about the Privacy Shield program, and to view these entities' certification, please visit www.privacyshield.gov.</p> <p>If some or all of the LNRS or RELX business is acquired by, another company personal data may be disclosed to the prospective or actual purchasers.</p>
<p>Third parties where required by law (or to protect our rights)</p>	<p>We also share personal data in order to:</p> <ul style="list-style-type: none"> • comply with the law; • investigate and help prevent security threats, fraud or other malicious activity; • enforce and protect the rights and property of LNRS or its affiliates; or • to protect the rights of our customers, employees and third parties. This may include sharing information for the purposes of crime prevention and fraud protection.

- ***How long we retain personal data***

We retain personal data as follows:

Category	Retention Period
<p>Identification data</p>	<p>We retain identification data (such as names and addresses) whilst there is a continuing need for us to utilise it. We keep this retention under review and we will remove data as and when we no longer require it.</p> <p>The faceprint, which is unique to an individual and is considered to be biometric data, will be stored for 24 hours.</p> <p>The photographic images will be stored securely by our Data Processors for as long as is needed to comply with applicable data protection laws and other regulatory obligations.</p>

--	--

How you can request to withdraw consent, access, correct, and delete or transfer your personal data or ask us not to process your personal data

In accordance with European and certain other privacy and data protection laws, as may be applicable, we provide you with the ability to exercise your rights in relation to your personal data in the following ways:

- ***Withdraw consent***

If you do not wish to use the App to complete an identity check you can refuse to consent and withdraw your consent at any time by contacting LNRS or by simply not using the App at all.

- ***Find out if we process your personal data, obtain a copy of the data or correct inaccurate data***

To find out if we process any of your personal data to access a copy of such personal data we may hold about you or correct any personal data that you believe is inaccurate, incomplete or out of date, you may contact us as provided in the “How to contact us” section below; You can also direct this request through the Client.

In order to provide you with an appropriate response we may ask for relevant identification documents to confirm your identity in handling your request and also send you a short form to complete to clarify the request and ensure it is dealt with efficiently and in accordance with data protection laws, as may be applicable. Where you dispute the accuracy of personal data we receive from third parties, we may confirm its accuracy with the third party that supplied it.

- ***How you can object to, or request to restrict, delete or transfer your personal data***

If you object to our processing of the personal data we may hold about you as a controller, or you wish to restrict our use of it or request its deletion, you may contact us as provided in the “How to contact us” section below. As stated above, we may also ask for relevant identification documents to confirm your identity in handling your request and also send you a short form to complete to clarify the request and ensure it is dealt with efficiently and in accordance with the European and certain other privacy and data protection laws, as may be applicable.

Your rights to object to, or request that we restrict our use of, or delete your personal data may be limited where we are legally required to process your personal data or have compelling reasons to overrule your request.

European and other privacy laws also give individuals a right to ask for information which they have given to a company, to be sent to other companies (for example you can ask for services managed online such as utilities, phone or email to be switched between providers). This is described as a “data portability” request. If you wish to apply this right, you may contact us as provided in the “How to contact us” section below.

How to contact us

If you have any questions or wish to exercise any of the rights described in this Privacy Notice, please contact our Data Protection Officer at Officer (at the following address) whom we have

appointed to respond to enquiries regarding any of the products connected to the data controllers described in this Notice:

Data Protection Officer
LexisNexis Risk Solutions Group
Global Reach
Dunleavy Drive
Cardiff
CF11 0SN
Email: DPO@lexisnexisrisk.com

If you have unresolved concerns, you have the right to complain to a data protection authority in the country where you live, where you work or where you feel your rights were infringed.

In the United Kingdom the relevant data protection authority are the Information Commissioner's Office (ICO):

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113
www.ico.org.uk

Last updated: April 2021