LexisNexis Risk Solutions - Business Services Processing Notice

Version 1.0 Last Updated: 24th May 2018

This Processing Notice contains the following sections:

- What this Processing 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 Processing Notice covers

This Processing Notice applies to services LexisNexis Risk Solutions ("**LNRS**", "**we**" or "**us**"), part of the RELX Group™ of companies, provides to business customers, local and national government bodies and other organisations (our "**Customers**") 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, assist them with the management and accuracy of their own customer records and accounts; and help them to trace individuals for legally necessary purposes such as debt collection, asset reunification and process serving.

These services are provided in the following categories to the extent they are subject to the European Union (EU) General Data Protection Regulation (GDPR):

Category	Product	Description
Identity and Fraud Management	IDU® InstantID® UK QA One Time Password Smartcleanse® Smartlink TraceIQ® TrueID®	These services help our Customers in a broad range of sectors, including finance, retail and government services to confirm your identity and to prevent and detect fraud and other potential offences.
Financial Crime Compliance	Bridger Insight® XG EDD Insight World Compliance™ Data World Compliance™ Online Search Tool	These services help our Customers who work in financial services and other industries to comply with regulations that require them to screen you and other clients to enable them to prevent and detect fraud, money laundering, bribery and corruption, and other potential offences.

Customer Data Management	Email Match TraceIQ® Smartcleanse® Smartlink Phone Match®	Through the provision of these services we assist our Customers with the ongoing maintenance of their relationship with you and their other clients. This could include activities designed to support data accuracy by cleansing and updating existing records, correcting database errors and identifying if you have recently moved, or if there is a recent change in your personal details or circumstances that may affect their relationship with you, including where you may be at financial risk.
Tracing and Investigations, Collections and Recovery	Collect Email Match Phone Match® Smartcleanse Smartlink TraceIQ®	These services support tracing and investigations, collections and recovery, where there is a legitimate interest in our Customers conducting activity to locate and contact you and other clients, to recover a debt, or to reunite, or confirm an asset is connected with, the right person.

Life and Pensions Existence/Mortality Checks, Asset Reunification and De-Risking	Existence Email Match Forensic Trace Mortality Phone Match® Risk MSP Smartlink Smartcleanse® TraceIQ®	These services are specifically developed and tailored to assist our Customers in the life and pensions industry to comply with regulations requiring them to keep your records fully up-to-date in accordance with the Pension Regulator's record-keeping guidance. This is an important requirement for all pension scheme and life assurance providers to help them ensure they are able to stay in contact with you or any of your family or close associates who may benefit now, or in the future from the provision of such a financial asset. In order to ensure that pension and life assurance assets are administered efficiently our services also used by our Customers to predict associated liabilities and risks to strengthen actuarial projections.

- ***How to know which services our Customers use***

The business or other organisation that is using our services for any of the relevant purposes outlined will be able to tell you which of our services (if any) they used in the course of the processing they have undertaken.

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

The LNRS group of companies controls the personal data we use in providing these services to our Customers. For more information on which LNRS company is the controller for each product, please see the "How to contact us" section below.

Our Customers who use our services are also data controllers. Their processing notices will tell you more about how they use personal data.

How we use personal data

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

We use personal data to help our Customers 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 prevent and investigate fraud and other potential offences, to assist them with the management and accuracy of their own customer records and accounts; and help them trace individuals for legally necessary purposes such as debt collection, asset reunification and process serving. We also use personal data to develop and improve our products and services.

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.

Where we use personal data for a business or other interest, data protection law says that we have to make sure this interest is legitimate and we must make sure we can justify any impact on individuals. To help us do this, we regularly update our databases to ensure they are accurate; we test our statistical models to check for errors or inaccuracy; we only collect information and provide it to Customers who can demonstrate they need it in order to provide you with their own service or product under a contractual agreement with you, to comply with certain regulatory requirements in their dealings with you as a client, or as necessary for their own legitimate interests. Even where a Customer can demonstrate this need, we limit such Customer access only to the types of personal data that are relevant for the specific interest in question.

We have set out more information about the legitimate business or other interests in processing personal data below:

Purpose	**How is personal data used and why?**
Enabling our Customers to verify your identity, age, residence, and prevent and investigate fraud, and assess risk	When you apply for services from credit, insurance or utility providers, retailers, government bodies and agencies, or other organisations they might ask you to provide identification and answer certain questions. Our products allow our Customers to check this information against our databases to confirm that you are who you say you are. For example, the Customer may check your name and address against addresses we have obtained from public sources, like the Electoral Register. In some cases, the output from a check will be 'yes' or 'no'; in other cases we may provide the likelihood that this is the same information (for example, by saying there is a high,

	medium or low chance this is the same person as the person on the Electoral Register).
Allowing our Customers to comply with regulatory requirements	Our products allow our Customers to check whether doing business with a client or potential client could create a risk of financial crime, such as bribery, corruption or money laundering. For example, when you apply for financial products, organisations may search your name against sanctions lists, watch-lists, lists of politically exposed persons, media reports and other publicly-available information in order to comply with their regulatory requirements. As such searches can return information relating to other individuals with similar names, our products provide scores to our Customers to help them identify the likelihood that a given record corresponds to you. For example, if a search identifies a news story indicating corruption by someone with a similar name to yours but located in a different area, our products will allow our Customers to understand the likelihood this is a match and whether to investigate further and determine for themselves any actions they are legally required to take.
Helping our Customers better manage their client accounts and records	We supply information including personal data to our Customers to help them maintain of their relationships with you and their other clients. This could include helping them remove inaccurate records (e.g. email addresses that are mistyped), and updating existing records, correcting database errors and identifying if you have recently moved. It could also include helping our Customers identify a recent change in your personal details or circumstances that may affect their relationship with you. For example, if a Customer has previously assessed your credit-worthiness, some of our products would allow them to identify a change in your circumstances that indicate you may be at financial risk.

Assisting Customers with their tracing, investigations, collections and recovery activities	We supply information including personal data to assist our Customers with their tracing (i.e. locating individuals), investigations, collections and recovery activities. Our products provide contact and address information to help our Customers locate individuals that owe debt and have moved or gone away and from whom they have no longer been able to collect payments for services. At the same time as locating individuals who may owe certain debts, our products and services also allow our Customers to confirm if an individual might be facing financial hardship, and where appropriate come to an agreed repayment plan in support of the ongoing client relationship. Such activities can often be performed in support of regulatory requirements such as the prevention or investigation of fraud, or to assist businesses and other organisations undertaking tasks in support of the substantial public interest.
Enabling life and pensions providers to undertake existence/mortality checks, asset reunification and de-risking activities	Where you or your spouse have a pension or life assurance plan, our Customers are required under law to ensure they have accurate and up-to date records for you, to ensure they can make maintain contact with you and provide you with important information about these significant long-term financial assets and benefits. These services also help our Customers to verify identity and prevent fraud through regular existence and mortality screening, by confirming if you are present at your current address, have moved to a new address or have been recently deceased.
Developing our statistical models, analytics and profiling	We use personal data for statistical models, analytics and profiling to improve our products and services and to help Customers better predict risk, to verify data you provide, to help prevent and investigate fraud, to allow them to comply with their regulatory requirements, to better manage their client accounts and records and assist them with their tracing, investigations,

	collection and recovery, asset reunification and de-risking activities. To do this, we compare information received against variables like name, age and address so our Customers can more accurately predict risk factors associated with their proposed or ongoing relationships with you.
Protecting our legitimate business interests and legal rights	Where we believe it is necessary to protect our legal rights, interests and the interests of others, we use personal data in connection with legal claims, compliance, regulatory, and audit functions, and disclosures in connection with the acquisition, merger or sale of a business.

- ***Where required by law***

In exceptional circumstances, we may be required by law to provide personal data to law enforcement agencies, courts or others in connection with claims and other litigation.

- ***Sensitive personal data***

Where the personal data we process includes sensitive or criminal offence data (as defined by the relevant law), we are able to process this data because it is necessary for a legal obligation, there is a substantial public interest or the information was manifestly made public.

What data is collected and from whom it is obtained

Our services depend on collecting accurate and up to date personal data. We obtain this data from the following sources:

- ***Credit Reference Agencies ("CRAs")***

We obtain personal data from CRAs, which includes:

Data used to identify and verify individuals, including:	• Name, current and previous addresses, date of birth, telephone contact information and individual identifiers, including from the Electoral Register and other publicly-available databases; and • Information as set out above relating to spouse, associate, children and other family members;
Credit header activity history, including:	• Confirmation of credit activity history such as number of accounts or other agreements that involve a credit arrangement – bank, mortgage, credit cards, utilities and communications (including mobile and internet);
Court judgments, bankruptcies, administrative orders and other public records, maintained by Registry Trust Ltd:	• Information about any bankruptcy or insolvency proceedings; and • Court judgments information - the name of the court, the nature of the judgment, how much money was owed, and whether the judgment has been satisfied.
Data concerning credit file searches:	• CRAs provide us with records they maintain each time an organisation makes an enquiry about an individual called a "search footprint", including the name of the organisation that made the enquiry, the date, and the reason they gave for making the enquiry.

The CRAs from which we receive personal data are Experian Limited, Equifax Limited, and Crediva Limited. For more information on how the CRAs collect and process personal data, please see:

http://www.experian.co.uk/crain

https://www.equifax.co.uk/crain

http://www.crediva.co.uk/crediva-processing-notice*

- ***Public and publicly-available records***

We receive the following personal data from public and publicly-available sources, including news and business information, and other third party sources. This includes data providers, biographical sources, broadcast content providers, social media providers and public source information such as government watch and sanction lists, or data provided under open government licence. Such source materials will often contain personal information, and where this is the case that personal information will also appear in our products and services, provided to our Customers in accordance with their relevant legitimate interest or requirement. Such records may include:

Source	Categories of personal data we receive
County and High Court Judgments, such as provided by Registry Trust	Information on court judgments that have been issued, such as how much money was owed and whether the judgment has been satisfied;
Identity and Passport Service - General Register Office (GRO)	Birth, marriages and death records and certificates and Disclosure of death registration information (DDRI);
Registered commercial entity information, such as Companies House	Data on directorships, such as presence of a director within a postcode area;
Property related information, such as Her Majesty's Land Registry (HMLR) – Property Register	Along with the address and postcode we receive information such as property type, age of property, tenure and sale prices;
Politically Exposed Persons (PEP) lists	Names of individuals in prominent public functions that present a higher risk for involvement in bribery or corruption, as defined under the Financial Action Task Force Recommendations; or close associates of PEPs, details of family circumstances, such as marital status and dependents, and in limited circumstances passport details. Position or affiliation within government; and family members and other related individuals.
Sanction lists	Names of individuals that have been sanctioned by governmental and supra-national authorities (such as the

	United Nations); details of the reasons for which sanctions are imposed; and affiliated businesses and associates.
Watch lists	Names of individuals placed on criminal watch lists, such as national and international terrorism watch lists; details of the alleged offenses; and affiliated businesses and associates.
Enforcement lists	Names of individuals provided by financial enforcement agencies; details of the alleged offenses; and affiliated businesses and associates.
Public media sources and publicly-available information from internet searches and websites	Information relating to individuals in published news sources such as name, age, date of birth, gender, country of residence; information from other public websites and social media, such as employment and education details, which may include details of public, religious, political or trade union roles; personal and professional affiliations; and, to the extent it appears in public search, information that may reveal connections to investigated, indicted, suspected of, or convicted for, criminal activity or offences which is considered a pre-cursor to money laundering or terrorist financing (e.g. arms trafficking, smuggling or fraud).

- ***LexisNexis® Risk Solutions data partners and service providers***

We also receive personal data from our data partners and service providers:

Source	**Categories of personal data we receive**
Third-party data partners and service providers	We receive data from trusted commercial sources and service providers in connection with the provision of our

	products which includes personal data such as name, current and previous addresses, postcodes, gender, date and place of birth, telephone and email contact, social media handles, professional status and background, financial account numbers for data for verification purposes; and other individual identifiers. This includes British Communications plc, Royal Mail plc, Vocalink Ltd and other commercial providers of similar data or services.

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 European Economic Area ("**EEA**"), we safeguard the data as described below.

Category	Description
Businesses, government bodies and other organisations	We share personal data with Customers when they check a client or potential client against our databases. We ask our Customers to explain to their clients that they use our information, including data provided to us by third parties. Where we share personal data with our Customers, including their affiliates or sub-contractors located in countries outside of the EEA, we make use of the EU-U.S. Privacy Shield Framework, European Commission-approved standard contractual data protection clauses, binding corporate rules for transfers to data processors (approved under Article 46(2)(b) of the General Data Protection Regulation), and other appropriate legal mechanisms to safeguard the transfer.
Credit Reference Agencies (CRAs) and Fraud Prevention Agencies (FPAs)	We share personal data with CRAs when we send them data from our Customers through some of our products and services that they check against their databases. We ask our Customers to explain to their clients that we provide this information to them and which we may be further used for identity verification, fraud prevention, debt collection, tracing and asset reunification purposes. If we or our Customers believe a fraud has been or might be committed, we may also share that data with FPAs such as CIFAS who collect, maintain and share data on known and suspected fraudulent activity. Most CRAs also act as FPAs.

Service providers and data partners	We share personal data with service providers who assist us with the provision of our products and services. These providers include data partners, customer support, IT service providers, financial services and professional advisors. Where we share personal data with service providers in countries outside of the EEA, we make use of the EU-U.S. Privacy Shield Framework, European Commission-approved standard contractual data protection clauses, binding corporate rules for transfers to data processors (approved under Article 46(2)(b) of the General Data Protection Regulation), and other appropriate legal mechanisms to safeguard the transfer.
Resellers, distributors, integrators and agents	We sometimes use other organisations to help provide products and services to clients and we may provide personal data to them in connection with that purpose.
Other affiliated companies of LexisNexis® Risk Solutions within the RELX Group of companies	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. These affiliates are located in the United Kingdom, Israel the Republic of Ireland and the United States. Where we share personal data with LNRS affiliates in countries located in countries outside of the EEA, we make use of the EU-U.S.

	Privacy Shield Framework, European Commission-approved standard contractual data protection clauses, binding corporate rules for transfers to data processors (approved under Article 46(2)(b) of the General Data Protection Regulation), and other appropriate legal mechanisms to safeguard the transfer. 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.
Third parties where required by law (or to protect our rights)	We also share personal data in order to: • 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
Sanctions lists, watch lists, PEP lists, adverse media searches, social media and other public website data	We retain information relating to sanctions, criminal records, adverse media searches as well as the information we obtain from social media and other public websites for such periods as necessary for our Customers to perform and comply with their financial crime compliance requirements. This is usually for a minimum period of 6 years but may be longer, depending on their location and relevant national laws.

Identification data	We retain identification data (such as names and addresses including from the Electoral Register) 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.
Credit Reference Agency (CRA) records	Data provided to us by credit reference agencies is subject to the retention periods determined by the relevant CRA, and subject to further agreed contractual provisions, applicable regulatory requirements and industry standards. Search footprints are retained by CRAs for different lengths of time. Experian and Equifax retain most search footprints for one year from the date of the search, although they keep debt collection searches for up to two years. Crediva keeps search footprints for two years from the date of the search.
Court judgments, bankruptcies, administrative orders	We retain information about court judgments or orders for up to 6 years from the date of the judgment or order (or a shorter period if the judgment is set aside or repaid). For bankruptcy, IVAs or other insolvency related events and arrangements, we usually keep such data for up to 6 years (or, if such events are extended, then for that longer period).
Other third party-supplied data and services	Other third party supplied data is retained as necessary for our Customers to perform and undertake their legitimate interests and activities, including those undertaken in the substantial public interest. The criteria used to determine the storage period will include the legal limitation of liability period, agreed contractual provisions, applicable regulatory requirements and industry standards.

Archived data	We may hold data in an archived form for longer than the periods described above, for things like research and development, analytics and analysis, (including refining fraud strategies, scorecard development and other analysis such as de-risking), for audit purposes, and as appropriate for establishment, exercise or defence of legal claims. The criteria used to determine the storage period will include the legal limitation of liability period, agreed contractual provisions, applicable regulatory requirements and industry standards.

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

In accordance with the General Data Protection Regulation (the "**GDPR**"), we provide you with the ability to exercise your rights in relation to your personal data in the following ways:

- ***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. 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 the GDPR. 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 your 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 GDPR.

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 override your request.

The GDPR also gives 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 manged online such as utilities, phone or email to be switched between providers). The GDPR describes this as a "data portability" request. As we don't collect information directly from individuals, this right does not apply to the personal data used in our services.

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.

How to contact us

If you have any questions or wish to exercise any of the rights described in this Processing Notice, please contact our Data Protection 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
Global Reach
Dunleavy Drive
Cardiff
CF11 0SN
Email: DPO@lexisnexisrisk.com

The data controller for each LNRS product/service is described below:

Services	Data controller
Collect Email Match Existence Forensic Trace Mortality Phone Match® Risk MSP Smartcleanse® Smartlink TraceIQ®	Tracesmart Ltd, trading as LexisNexis*
Bridger Insight® XG EDD Insight IDU® InstantID® UK QA One Time Password	Tracesmart Ltd, trading as LexisNexis* LexisNexis Risk Solutions UK Ltd*

TrueID®	LexisNexis Risk Solutions FL Inc.*, represented in the EU by its affiliated company LexisNexis Risk Solutions UK Ltd* World Compliance Inc.*, represented in the EU by its affiliated company LexisNexis Risk Solutions UK Ltd*
WorldCompliance™ Data WorldCompliance™ Online Search Tool	World Compliance Inc.*, represented in the EU by its affiliated company LexisNexis Risk Solutions UK Ltd*

*Tracesmart Ltd, trading as LexisNexis, LexisNexis Risk Solutions UK Limited, LexisNexis Risk Solutions FL Inc, World Compliance Inc., and Crediva Ltd are part of the LexisNexis Risk Solutions unit in the RELX Group of companies.