LexisNexis Risk Solutions – Processing Notices

LexisNexis Risk Solutions Group ("**LNRS**", "**we**" or "**us**") provides our business customers with tools that permit them to analyse and predict risk in a number of different business sectors. For example, some of our products help insurer's price motor insurance policies, while others assist financial institutions and other businesses in complying with anti-money laundering regulations, identity management, fraud prevention and investigation, and tracing for debt collection and asset reunification purposes. Many of these tools rely on personal data that we obtain from public sources and other non-publicly-available sources. Our Processing Notices give more information about this. They also explain the sources from which we obtain personal data as well as the rights individuals have to access their personal data, correct inaccurate data and to object to our use of personal data for these purposes.

For more information about our business lines, please consult the Processing Notices listed below.

- Insurance Services
- Business Services
- ThreatMetrix
- Emailage

Lexis Nexis Risk Solutions Group - Emailage Processing Notice

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 offered by Emailage Corp. ("**Emailage**", "**we**", "**us**"), a LexisNexis Risk Solutions Group company, part of the RELX Group™ of companies.

Emailage provides identity validation and risk assessment services to business customers (our "**Customers**") who interact and enter into transactions with individuals. Our services are designed 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 to prevent and investigate fraud and other potential offences; to reduce fraud in the market; and to improve customer experiences and drive transaction approvals. Our services also benefit individual customers, prospective customers and the public generally, as the cost of fraud is one of the factors that can push up the costs of products and services.

If you procure goods or services from one of our Customers (or seek to enter into transactions with them) they may use our services to help them check that you are who you say you are, and that the contact information you provided is yours. This is all done in near "real time" behind the scenes, and our Customer chooses how they use our services and risk assessment (together with other checks they might perform) as part of their fraud prevention and due diligence checks.

If you have been provided with our details by one of our Customers, or a link to this processing notice, that is because our Customer has asked us to provide a risk assessment on the details you provided, and we have asked them to ensure that you are made aware of how we use your personal information to provide our services to them.

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

Emailage controls the personal data we use in providing these services to our Customers. 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 to prevent and investigate fraud and other potential offences; to reduce fraud in the market; and to improve customer experiences and drive transaction approvals. 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 you or a particular client is solely up to them. The personal data or scores 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.

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, prevent and investigate fraud, and assess risk	When you apply for services from credit, insurance or utility providers, retailers, or other organisations they might use our services to help them check you are who you say you are, and that the contact information you provided is yours. Our products allow our Customers to evaluate fraud risk in near real time. For example, when opening a new account or processing an online transaction, a Customer may process your email address and IP address through our service to generate a fraud risk score. Emailage generates a fraud risk score by matching and evaluating the supplied data points to associated meta data (email data, email domain data, IP geolocation data) and previous Customer queries and fraud indicators contributed to Emailage's global fraud network. Using our fraud risk score together with other checks they might perform, a Customer can assess risk associated with the application or transaction and make decisions in an effort to identify and prevent fraud (e.g., manually review a high-risk transaction before approving).
Allowing our Customers to comply with regulatory requirements	Our services form part of our Customers' compliance checks, which are necessary for them to ensure they meet external and internal governance obligations (including necessary risk due diligence on individual customers and potential customers).

	In particular, our Customers have a legitimate interest in verifying the identity of its individual clients and verifying the information they provide when they engage with clients. Our services forms part of this verification process, by providing a fraud risk score and digital identity score in relation to the individual client's personal information.
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 to prevent and investigate fraud, to allow them to comply with their regulatory requirements. To do this, we compare information received against variables like name, email address, postal address, phone number, device ID, IP address, and other transaction-level details to provide our Customers with a fraud risk score and digital identity score so they 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***

Emailage does not process sensitive or criminal offence data (as defined by the relevant law); however, in the event such data was processed we would be 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:

- ***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, email

	address, email domain, IP address, postal address, Bank Identification Numbers (BIN), gender, date of birth, telephone, social media handles, professional status and background

- ***Our Customers***

We also receive personal data from our Customers:

Source	Categories of personal data we receive
Our Customers	Our Customers choose which personal data of their clients and prospective clients to send to us when using our service which includes personal data such as name, email address, IP address, phone number, billing address, shipping address, device ID, Bank Identification Number (BIN), hashed card number, transaction information (e.g. amount, currency), service information (e.g. service date, location, type). We also receive fraud feedback data from our customers which indicates whether previous transactions processed through our service were determined to be fraudulent.

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
Businesses and other organisations	We share personal data with Customers when they check a client or potential client using our service. We ask our Customers to explain to their clients that they use our information, including data provided to us by third parties. 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.
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. 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.
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 within the LexisNexis® Risk Solutions and RELX Group of companies	Some of the service providers we use are other affiliated companies within the LexisNexis Risk Solutions Group and 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 products or services. 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 Australia, Brazil, France, Germany, Iceland, India, Italy, Ireland, the Netherlands, the Philippines, Singapore, South Africa, 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. 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. If some or all of the LexisNexis Risk Solutions Group 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 our rights and property and those of our 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
Identification data	We retain identification data 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.
Customer enquiry data	We retain personal information associated with and resulting from our customer enquiries or checks whilst it continues to be relevant to our services and 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.
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 defense 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 European and other privacy laws, 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 European and other privacy laws. 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 privacy laws.

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.

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 manged online such as utilities, phone or email to be switched between providers). This is described as a "data portability" request. In some instances, this right may not apply to the personal data we process.

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 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

Last updated: 21st April 2021