RELX DATA PRIVACY FRAMEWORK NOTICE

(Last updated October 1, 2024)

COVERED ENTITIES

The following RELX U.S. entities ("we," "us" or "our") have certified to the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework programs (collectively, "DPF") as set forth by the U.S. Department of Commerce:

Elsevier Inc.
LexisNexis, a division of RELX Inc.
LexisNexis Risk Data Management LLC
LexisNexis Risk Holdings Inc.
LexisNexis Risk Solutions FL Inc.
LexisNexis Risk Solutions Inc.
LNRS Data Services Inc.
Reed Elsevier Technology Services, a division of RELX Inc. ("RETS")
Threatmetrix, Inc.
WorldCompliance Inc.

Our DPF certification is listed here: www.dataprivacyframework.gov.

SCOPE

We adhere to the DPF Principles including relevant Supplemental Principles (collectively, the "Principles") with respect to the processing of personal data received in reliance on the relevant parts of the DPF provided by customers and their authorized users, clients, agents and service providers in the European Economic Area, the United Kingdom (and Gibraltar), and Switzerland under contract with us or our affiliates or resellers for the following online services:

- Elsevier Entellect, Funding Institutional, Pure and Shadow Health services
- LexisNexis Legal & Professional services provided by LexisNexis, a division of RELX Inc.
- LexisNexis Risk Solutions analytics, claims, compliance, credit risk, customer acquisition, data management, fraud prevention, identity verification, payments and risk management solutions
- LNRS Data Services Cirium (including FlightStats), ICIS and Brightmine services
- Our services supported by RETS

If there is any conflict between the terms in this RELX Data Privacy Framework Notice and the Principles, the Principles shall govern.

TYPES OF PERSONAL DATA COLLECTED

The types of personal data collected from customers and their authorized users, clients, agents and service providers, depending on the service, includes their contact and registration information, client and prospect information, including account and device data, financial and billing information, claims processing data, clinical records, research data, security authorization, identification and authentication data, transactional data, usage activity, preferences and other personal data they provide.

PURPOSES FOR PERSONAL DATA COLLECTION AND USE

We collect and use such personal data to provide and improve our services, customer and technical support, and billing and marketing activities, to respond to requests, to process transactions, for administrative purposes and as otherwise instructed by customers and their authorized users, clients, agents and service providers.

DISCLOSURES TO THIRD PARTIES

We disclose such personal data to the following types of third parties for the foregoing purposes:

- Affiliates, contractors, service providers and other third parties to assist us in providing our services, support and related activities to customers based on our instructions;
- Customers' affiliates and their administrators and other authorized recipients as part of the customer group's subscription to our services or as otherwise instructed by customers;
- Business partners, sponsors and other third parties with which we offer webinars, white papers, applications and other services;
- Channel partners, such as distributors and resellers, to fulfill product and information requests;
- Other corporate entities as part of a business transition, such as a merger, acquisition by another company, or sale of all or a portion of our assets.

We remain responsible for the personal data that we share with third parties for processing on our behalf, and we remain liable under the Principles if such third parties process such personal data in a manner inconsistent with the Principles and we are responsible for the event giving rise to the damage.

We may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

RIGHTS OF ACCESS AND LIMITING USE AND DISCLOSURE

Individuals have a right to access to their personal data, to correct, amend, or delete that data, and to limit use and disclosure of that data, subject to certain exceptions. To exercise these rights, please contact us via the contact details below. Please note that where we are processing personal data for our customer, we may first refer your request to the customer that submitted your personal data, and we will assist our customer as needed in responding to your request.

INQUIRES OR COMPLAINTS

If you have any inquiry or complaint concerning this RELX Data Privacy Framework Notice or our participation in the DPF, please contact the RELX Privacy Office at privacy@relx.com or

Privacy Office
RELX
P.O. Box 933
Dayton, Ohio 45401
USA

If the issue cannot be resolved through our internal processes, you may file a claim free of charge with JAMS, an independent U.S. alternative dispute resolution provider, at http://www.jamsadr.com/eu-us-data-privacy-framework. If you have a complaint left unresolved by all available recourse mechanisms, you may invoke binding arbitration. For more details, visit https://www.dataprivacyframework.gov/program-articles/How-to-Submit-a-Complaint-Relating-to-a-Participating-Organization%E2%80%99s-Compliance-with-the-DPF-Principles.

ENFORCEMENT

Our commitments under the DPF are subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.