Event Data Processing Addendum

Last updated: 1 January 2025

This Event Data Processing Addendum ("DPA") forms part of the agreement (“Agreement”) between the RELX entity and the sponsor, exhibitor or other party (each, a “Party”) specified in the Agreement in which this DPA is referenced.

1. Definitions

1.1 “Data Protection Laws” means all applicable privacy and data protection laws, rules, regulations, decrees, orders and other government requirements.

1.2 The terms “controller”, “data subject,” “joint controller,” “personal data” and “processing” will have the same meanings ascribed to them in the Data Protection Laws, and where the Data Protection Laws use equivalent or corresponding terms, such as “personal information” instead of “personal data,” they will be read herein as the same.

2. Scope

2.1 This DPA applies to the processing of personal data each Party receives from the other and, if applicable, its affiliates under the Agreement.

2.2 The nature and purpose of the processing is in connection with the exhibition, show, conference, webinar, seminar or other event and related services under the Agreement. The duration of the processing is in accordance with the Agreement. The categories of personal data processed are those processed under the Agreement. The categories of data subjects are those whose personal data is processed under the Agreement.

3. Roles and Restrictions

3.1 Each Party independently determines the purposes and means of its processing of personal data and, therefore, each Party is an independent controller of the personal data. The Parties do not and will not process the personal data as joint controllers.

3.2 Each Party will comply with its obligations under the Data Protection Laws, and each Party will be individually and separately responsible for its own compliance. Nothing in this DPA will modify any restrictions applicable to either Party’s rights to process the personal data under the Agreement.

4. Assistance

4.1 Each Party will cooperate with and assist the other as reasonably required to enable the other Party to comply with its obligations under the Data Protection Laws, taking into account the nature of processing and the information available to the Party.

5. Cross-border Transfer

5.1 Each Party will ensure that, to the extent that any personal data is transferred by the Party to another country, such transfer will be subject to appropriate safeguards that provide an adequate level of protection in accordance with the Data Protection Laws.

6. Jurisdiction-Specific Terms

6.1 To the extent that either Party is processing any personal data originating from or otherwise subject to the Data Protection Laws of any of the jurisdictions listed below, the terms specified therein with respect to the applicable jurisdiction(s) apply in addition to the foregoing terms.

European Economic Area, United Kingdom and Switzerland

1. To the extent that either Party transfers personal data from the European Economic Area ("EEA"), the United Kingdom ("UK") or Switzerland to the other Party located outside the EEA, UK or Switzerland, unless the Parties may rely on an alternative transfer mechanism or basis under the Data Protection Laws, the Parties will be deemed to have entered into the standard contractual clauses approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 available at http://data.europa.eu/eli/dec_impl/2021/914/oj ("Clauses") in respect of such transfer, whereby:

a. the receiving Party is the "data importer" and the other Party is the "data exporter";

b. Module One applies, Modules Two, Three and Four, the footnotes, Clause 11(a) Option and Clause 17 Option 2 are omitted, and the applicable annexes are completed respectively with the information set out in the DPA and the Agreement;

c. the "competent supervisory authority" is the supervisory authority in the country where the data exporter is established;

d. the Clauses are governed by the law of the country where the data exporter is established;

e. any dispute arising from the Clauses will be resolved by the courts of the country where the data exporter is established; and

f. if there is any conflict between the terms of the Agreement and the Clauses, the Clauses will prevail.

2. In relation to transfers of personal data from the UK, the Clauses as implemented under section 1 above will apply as modified by the International Data Transfer Addendum to the EU Standard Contractual Clauses issued under Section 119A(1) Data Protection Act 2018 available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf ("UK Addendum"), with tables 1 to 3 completed respectively with the information set out in the DPA and the Agreement and table 4 completed by selecting "neither party".

3. In relation to transfers of personal data from Switzerland, the Clauses as implemented under section 1 above will apply subject to the following modifications:

a. references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss Federal Act on Data Protection ("FADP");

b. references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the FADP;

c. references to "EU", "Union", "a Member State" and "Member State law" shall be replaced with references to "Switzerland" or "Swiss law", as applicable;

d. the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of accessing their rights;

e. Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the Swiss Federal Data Protection Information Commissioner;

f. the Clauses are governed by the law of Switzerland; and

g. any dispute arising from the Clauses will be resolved by the courts of Switzerland.

Latin America

LATAM Addendum

Middle East and Africa

MEA Addendum

United States

1. To the extent that either Party sells to or shares with the other Party any personal information in scope of the California Consumer Privacy Act and its implementing regulations ("CCPA"):

a. The purposes for which the personal information is made available to the receiving Party is as set forth in the Agreement and subject to its privacy policy;

b. The personal information is made available to the receiving Party only for the limited and specified purposes set forth in the Agreement and is required to be used only for those limited and specified purposes;

c. The receiving Party is required to comply with applicable sections of the CCPA, including – with respect to the personal information that is made available to the receiving Party – providing the same level of privacy protection as required of businesses by the CCPA;

d. The disclosing Party is granted the right – with respect to the personal information that is made available – to take reasonable and appropriate steps to ensure that the receiving Party uses the personal information in a manner consistent with the disclosing Party's obligations under the CCPA;

e. The disclosing Party is granted the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information made available to the receiving Party; and

f. The receiving Party is required to notify the other Party after it makes a determination that it can no longer meet its obligations under the CCPA.