THOMSON REUTERS DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") amends the Agreement between Thomson Reuters and Customer, and sets out the obligations of both parties with respect to the Processing of Customer Personal Data in connection with the Agreement. Unless otherwise defined herein, any capitalized terms shall have the meanings given to them in the Agreement.

1. DEFINED TERMS. The following terms shall have the following meanings in this DPA:

1.1. **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "**Control**," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2. "**Agreement**" means the underlying agreement between Thomson Reuters and the Customer for the provision of the Services that references and incorporates this DPA;

1.3. "**Applicable Data Protection Law**" means data privacy and cybersecurity laws to the extent applicable to the relevant party's Processing of Customer Personal Data;

1.4. **"Authorized Affiliate"** means any of Customer's Affiliate(s) which (a) is subject to Applicable Data Protection Law, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Thomson Reuters, but has not signed its own Agreement or Order Form with Thomson Reuters and is, therefore, not a "Customer" as defined under this DPA.

1.5. "**Customer**" means the legal entity which has directly entered into the Agreement for Services with Thomson Reuters or its Affiliates;

1.6. "**Customer Personal Data**" means the Personal Data that Customer or its Authorized Affiliate provides under the Agreement for Thomson Reuters to Process on behalf of Customer in connection with the Services. Customer Personal Data does not include information that is (i) deidentified, anonymized, aggregated, publicly available information, or business contact data (unless the Applicable Data Protection Law otherwise considers such information as Personal Data), (ii) Usage Statistics; or (iii) any information that the Applicable Data Protection Law specifically states does not constitute Personal Data;

1.7. "**Security Breach**" means a confirmed breach of security that results in the unauthorized destruction, loss, alteration, disclosure of, or access to Customer Personal Data where such breach of security is likely to result in a significant risk of harm to a Data Subject(s) or where Thomson Reuters is required by Applicable Data Protection Law to notify Customer thereof;

1.8. "**Services**" means the products or services provided by Thomson Reuters to Customer pursuant to the Agreement.

1.9. "**Standard Contractual Clauses**" means those model clauses approved pursuant to Applicable Data Protection Law that legitimizes the transfer of Personal Data across borders, including the Standard Contractual Clauses approved by the European Commission which can be found *here*;

1.10. "**Subprocessor**" means a subcontractor providing Services where such subcontractor Processes Customer Personal Data.

1.11. "**Thomson Reuters**" means the named Thomson Reuters entity that has entered into the Agreement for Services with Customer;

1.12. "**Usage Statistics**" means information that is generated by or on behalf of Thomson Reuters and that is derived by or through the use of the Services.

1.13. "**Controller**" also referred to as "**Business**", "**Processor**" also referred to as "**Service Provider**", "**Data Subject**" also referred to as "**Consumer**", "**Personal Data**" also referred to as "**Personal Information**", "**Process**" or "**Processing**", and "**Sell**" or "**Selling**" (or any of their analogous terms) shall all have the meanings set out in the relevant Applicable Data Protection Law.

2. PROCESSING OF CUSTOMER PERSONAL DATA AND PARTIES' OBLIGATIONS

2.1. **Compliance with Laws.** Each party agrees to comply with its own obligations under Applicable Data Protection Laws.

2.2. **Parties' Obligations.** With respect to the Processing of Customer Personal Data in connection with the Services, the parties agree that:

2.2.1. Customer is the Controller of Customer Personal Data and, consequently, Thomson Reuters is a Processor thereof;

2.2.2. Each party will (i) inform the other if, in its reasonable opinion, an instruction infringes on its own obligations under Applicable Data Protection Law or other laws and (ii) upon reasonable request, provide assistance required under Applicable Data Protection Law with respect to data protection impact assessments, consulting with relevant data protection authorities, and/or making available relevant information necessary to demonstrate compliance with Applicable Data Protection Law;

2.2.3. Without limiting Section 2.1, Customer represents and warrants that it has obtained all consents for and rights to, and has provided all necessary notices to Data Subjects with respect to, the Customer Personal Data as required for the same to be Processed as contemplated by the Agreement; and

2.2.4. Except as required under Applicable Data Protection Law, Customer acknowledges and agrees that Thomson Reuters is under no duty to independently collect consent from or provide notice to any Data Subjects or to investigate the completeness, accuracy, or sufficiency of any specific Customer instruction or Customer Personal Data.

3. OBLIGATIONS OF THOMSON REUTERS. Thomson Reuters will take steps to ensure that:

3.1. **Limitations on Processing.** It only Processes the Customer Personal Data hereunder in alignment with Customer's instructions, including those set forth in the Agreement;

3.2. **Personnel.** Its personnel (including staff, agents, and Subprocessors) who handle Customer Personal Data are subject to a duty of confidentiality;

3.3. **Security.** It maintains and implements appropriate technical and organisational measures designed to protect Customer Personal Data against unauthorized destruction, loss, alteration, disclosure thereof, or access thereto. The parties agree that the specific technical and organizational measures located on Exhibit A attached hereto are in scope and fulfill the obligations of this Section;

3.4. **Access Requests.** Thomson Reuters will provide reasonable cooperation to Customer or a Data Subject to fulfil a Data Subject's request to access, correct, delete, or cease processing of data. To the extent Thomson Reuters receives a request, correspondence, enquiry, or complaint from a regulator that directly relates to Customer Personal Data, then (to the extent permissible) it will promptly refer the same to Customer for handling;

3.5. **Breach Notification.** It will report a Security Breach within the time required by the Applicable Data Protection Law or by the Agreement and, to the extent known, shall provide relevant information and reasonable cooperation so that Customer can fulfil its own obligations as Controller. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users;

3.6. **Deletion and Retention.** Upon request, it will delete the Customer Personal Data in its (or its Subprocessors') possession, except to the extent that Thomson Reuters is required to retain such data by law or its data retention policies (in which case Thomson Reuters shall isolate and protect such Customer Personal Data from further active Processing except to the extent required by law);

3.7. **Subprocessors.** It will maintain, where required by Applicable Data Protection Law, an online listing of Thomson Reuters Subprocessors set forth on its webpages *here* or in notices provided from time to time; impose written data protection terms on any Subprocessor that are no less restrictive than the terms of this DPA; remain primarily liable for an acts or omissions of its Subprocessor in the same manner as for its own acts or omissions under the Agreement;

3.7.1. **Objection.** It will provide Customer the opportunity to reasonably object within 10 days of notice of the appointment or replacement of a Subprocessor, in which case and to the extent reasonable, Thomson Reuters will either give Customer an opportunity to pay for the Service without use of the objectionable Subprocessor or terminate, subject to the terms of the Agreement, the specific Service(s) affected by the Subprocessor at issue;

3.8. **Audits.** Upon Customer's written request and no more than once per year during the term of the Agreement, Thomson Reuters will allow for and contribute to audits conducted by Customer or an external auditor selected by Customer in the form of providing answers to a reasonable questionnaire with respect to Thomson Reuters's Processing of Customer Personal Data. At Customer's expense and to the extent a more extensive audit is granted by Thomson Reuters, then the parties agree to negotiate, in good faith, a statement of work that outlines the scope and time frames of the audit.

4. **DATA TRANSFERS.** Customer (or its agents) or Thomson Reuters will only transfer (including any onward transfers) Customer Personal Data as permitted by Applicable Data Protection Law. If Applicable Data Protection Law requires the participation of Thomson Reuters to legitimize the transfer, such as the execution of Standard Contractual Clauses, then Customer shall notify Thomson Reuters and the parties will cooperate in good faith to implement the required transfer mechanism. If Customer becomes aware of any data localization laws that require Thomson Reuters, as a Processor to Customer, to keep a primary or the sole copy of the Customer Personal Data in a certain country, Customer shall notify Thomson Reuters and the parties shall cooperate in good faith to determine how to appropriately comply with such requirements.

5. **GENERAL.** All other terms and conditions of the Agreement remain in full force and effect. In the event of any inconsistencies between this DPA and the Agreement, this DPA shall prevail as it relates to the Processing of Customer Personal Data only.

EXHIBIT A: THOMSON REUTERS DATA SECURITY ADDENDUM

1. INFORMATION SECURITY PROGRAM.

1.1. **Information Security Program.** Thomson Reuters will maintain an information security program designed to protect the confidentiality, integrity, and availability of Customer Personal Data. The program includes, but is not limited to, the following components:

1.1.1. Information security policy framework;
1.1.2. Program documentation;
1.1.3. Auditable controls;
1.1.4. Compliance records;
1.1.5. Appointed security officer and information security personnel.

1.2. **Policies, Standards, and Guidelines.** Thomson Reuters will establish and maintain information security policies, standards, and guidelines designed to protect the confidentiality, integrity, and availability of Customer Personal Data hosted in the Services, which includes the following:

1.2.1. Policies to restrict access to Customer Personal Data only to authorized Thomson Reuters personnel and subcontractors;
1.2.2. Policies requiring the use of unique user ID's and passwords;
1.2.3. Policies requiring secure connections to the internet to have commercially reasonable controls designed to detect and terminate unauthorized activity prior to the firewall maintained by Thomson Reuters;
1.2.4. Policies requiring performance of regular vulnerability assessments of Thomson Reuters LAN, WAN, and critical application and network components;
1.2.5. Policies for the use of anti-malware and patch management controls designed to protect against virus or malware infection and exploitation of security vulnerabilities;
1.2.6. Policies and standards for the use of auditable controls that record and monitor activity.

1.3. **Training.** Thomson Reuters will train and communicate to its personnel the defined information security principles and information security policies and standards, including that:

1.3.1. Thomson Reuters personnel will be trained in information security practices and the correct use of information processing facilities designed to minimize possible security threats;
1.3.2. Security awareness training attendance reports will be maintained in the Thomson Reuters personnel's file or other compliance tracking tool;
1.3.3. Thomson Reuters personnel will be required to report any observed or suspected threats, vulnerabilities, or incidents to the designated point of contact;
1.3.4. Thomson Reuters information security personnel will be made aware of reported information security threats and concerns, and will be equipped to support the Thomson Reuters information security policy in the course of their normal work.

1.4. **Access Controls.** Thomson Reuters will manage its personnel access to systems supporting the Services in a manner that is designed to be granted on a need-to-know basis consistent with assigned job responsibilities.

1.5. **Business Continuity.** Thomson Reuters will develop business continuity plans, in which these plans will be tested and approved by Thomson Reuters management on a periodic basis.

1.6. **Vendor Risk Assessment.** Thomson Reuters will maintain a program for vendor risk assessment.

2. **DATA SECURITY CONTROLS.** In the context of the Agreement, Thomson Reuters will use commercially reasonable efforts to:

2.1. **Application Strategy, Design, and Acquisition.**

2.1.1. Inventory applications and network components that support provision of hosted services and assess their business criticality;

2.1.2. Perform Thomson Reuters standard security compliance review for acquired or developed applications;

2.1.3. Review critical applications at least annually for compliance with industry and commercially reasonable security standards.

2.2. **Anti-Virus and Anti-Malware.**

2.2.1. Implement and configure anti-virus and anti-malware software for regular signature updates;

2.2.2. Implement threat management capabilities designed to protect systems holding or processing Customer Personal Data.

2.3. **Network Security.**

2.3.1. Configure network devices (including routers and switches) according to approved lockdown standards;

2.3.2. Govern and monitor changes to network security controls (including firewalls) using change management standards;

2.3.3. Segregate data center networks into separate logical domains with the network security controls approved by Thomson Reuters security personnel.