THOMSON REUTERS

# Supply Chain Data Protection Agreement

This Data Protection Agreement ("Agreement") is effective on the date of the last signature of the Agreement ("Effective Date"), between Thomson Reuters Holdings Inc. a Delaware Corporation with an office at 610 Opperman Drive, Eagan, Minnesota 55123 ("Thomson Reuters"), and the supplier identified in the signature block ("Supplier"). Thomson Reuters is executing this Agreement for the benefit of Thomson Reuters and all its Affiliates who are the data controllers, owners or licensees of Thomson Reuters Data that Supplier (or any Supplier Affiliate) processes on behalf of any such Thomson Reuters Affiliate in the course of providing products or services to Thomson Reuters.

## 1. Definitions.

Affiliate: An entity that, from time to time, directly or indirectly controls, is controlled by, or is under common control with a party, or that is a successor (including, without limitation, by change of name, dissolution, merger, consolidation, reorganization, sale or other disposition) to any such entity or its business and assets. An entity will be deemed to control another entity if it has the power to direct or cause the direction of the management or policies of such entity, whether through the ownership of voting securities, by contract or otherwise.

BCR: The binding corporate rules which Supplier and its Affiliates may be party to, and which are both internally and externally binding for the benefit of Data Subjects, and have been approved by all relevant regulators.

Data Protection Laws: All applicable laws, standards and regulations governing the Processing of Personal Information, as may be amended or enacted from time to time, including, but not limited to: the EU General Data Protection Regulation 2016/679 ("GDPR"); any national laws which implement the GDPR; the UK Data Protection Act 2018; the U.S. Health Insurance Portability and Accountability Act ("HIPAA"); the U.S. Gramm-Leach-Bliley Act ("GLBA"); the California Consumer Privacy Act of 2018 ("CCPA"); the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); the Australian Federal Privacy Act 1988 and Privacy Amendment (Enhancing Privacy Protection) Act 2012; the Swiss Federal Act on Data Protection ("DPA"); the Argentina National Constitution and The Personal Data Protection Law No. 25,326 ("PDPL") (and its regulatory presidential decrees); India's Information Technology Act 2000; Japan's Act on Protection of Personal Information ("APPI"); Brazilian Personal Data Protection Law ("LGPD"); the Payment Card Industry Data Security Standard ("PCI DSS"); any fair information practices for handling, storing or managing data with privacy, security, and fairness that are incorporated into the foregoing or any other applicable laws or regulations (including, but not limited to, the Australian Privacy Principles, PDPL imposed data protection principles, and any similar regulatory authority responsible for the enforcement of Data Protection Laws); and, where applicable, any guidance and codes of practice issued by any standards authority or government regulator or authority established in a particular jurisdiction which govern the Processing of Personal Information.

Data Subject Request: Any request by or on behalf of a unique person who can be identified, directly or indirectly, by Personal Information or to whom the Personal Information relates ("Data Subject") to exercise the rights afforded to them by Thomson Reuters (or its Affiliates) or by Data Protection Laws, including, but not limited to, the right to complain, right to receive contact information for the purposes of handling complaints, right to access, right to notice, right to deletion and/or right to be forgotten, right to opt out of certain Processing, and other rights.

EU Law: European Union law, and the law of any Member State of the European Union from time to time.

Metadata: Any non-content data that describes and gives information about Thomson Reuters Data as may be specifically defined by Data Protection Laws, including, but not limited to, traffic data, transmission data, and tracking data.

Order: The form or process by which Thomson Reuters acquires products or services from Supplier, which form could be a statement of work or other ordering document, and which may refer to a governing master agreement.

Personal Information: Any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Personal Information includes information that could reasonably be linked, directly or indirectly, or inferred, with a particular consumer or household.

Process (and its derivatives): Any operation or set of operations that is performed upon Thomson Reuters Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Sensitive Personal Information: Any Personal Information that requires additional protection under applicable Data Protection Laws as a result of its sensitive nature, including, without limitation, information concerning an individual's racial

or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, physical or mental health, sex life or orientation, criminal records, financial account numbers, account passwords or voice mail access codes, medical records, biometric and genetic information, date of birth and government-issued identification numbers (such as U.S. Social Security numbers or other national insurance or identification numbers, driver's license numbers, and passport numbers).

Thomson Reuters Data: All electronic data or information, including Metadata, submitted or made available by Thomson Reuters, its agents, customers, suppliers, contractors, and outsourcers to Supplier. Thomson Reuters Data includes Personal Information and Sensitive Personal Information.

**2. General.** Unless otherwise agreed by Thomson Reuters and Supplier, all Thomson Reuters Data is and shall remain the exclusive property of Thomson Reuters. Supplier shall Process Thomson Reuters Data only for the benefit of Thomson Reuters; only to the extent strictly necessary to perform its obligations under this Agreement or an Order, or as otherwise required by law (in such case upon prior notice to Thomson Reuters unless the relevant law prohibits giving notice on important grounds of public interest); and only in accordance with documented instructions contained in this Agreement or received from Thomson Reuters from time to time in writing.

Supplier may not otherwise use or modify the Thomson Reuters Data, merge it with other data, commercially exploit it, sell it, disclose it, transfer it across international borders or do any other thing that may, in any manner, adversely affect the integrity, security or confidentiality of such Thomson Reuters Data, other than as expressly specified herein or as directed by Thomson Reuters in writing.

Supplier shall not maintain a copy of any Thomson Reuters Data, and shall not otherwise remove or duplicate any Thomson Reuters Data hereunder except as allowed under this Agreement or by the express written permission of Thomson Reuters. Upon the Agreement termination and if requested by Thomson Reuters, Supplier shall return any Thomson Reuters Data under Supplier's care to the control of Thomson Reuters; or, if authorized and by providing a written certification of such, shall discard, destroy, and otherwise dispose of Thomson Reuters Data, making such data unrecoverable, in a secure manner to prevent unauthorized handling of the Thomson Reuters Data consistent with Thomson Reuters policies, applicable industry standards and/or applicable law.

Supplier may retain a copy of Thomson Reuters Data only to the extent it is obliged by EU Law (or in the case of data originating solely from outside of the European Union, only to the extent it is obliged to so by the laws of the country from which the relevant data originated).

**3. Data Security.** Supplier shall:

(i) implement and maintain current and appropriate technical and organizational measures to protect Thomson Reuters Data against accidental, unauthorized or unlawful Processing and against accidental loss, destruction, damage, alteration, disclosure or access;

(ii) have the following audited reports or certifications and annually provide to Thomson Reuters (i) its SSAE-16 report (or equivalent); (ii) its SOC 2 Type II report; (iii) its ISO 27001, ISO 27018, and ISO 9001 Statements of Applicability and certification; and (iv) an executive summary of that year's third party vulnerability assessment/penetration test of Supplier's systems and networks;

(iii) provide third-party attestation of static or dynamic application security testing or penetration testing on all software Processing Thomson Reuters Data, remediate any identified high vulnerabilities prior to delivery to Thomson Reuters, provide written remediation plans for medium and low vulnerabilities, and provide evidence of its remediation of any identified security vulnerabilities at Thomson Reuters' request;

(iv) take reasonable steps to ensure the integrity of any employees who have access to Thomson Reuters Data, including by conducting background checks in accordance with an Order or a governing agreement referenced by an Order;

(v) maintain a level of security appropriate to the harm that may result from any unauthorized or unlawful Processing or accidental loss, destruction, damage, denial of service, alteration or disclosure, and appropriate to the nature of Thomson Reuters Data;

(vi) oblige its employees, agents or other persons to whom it provides access to Thomson Reuters Data to keep it confidential in accordance with an Order or a governing agreement referenced by an Order;

(vii) provide annual training to staff and subcontractors on the security requirements contained herein;

(viii) maintain measures designed to ensure the ongoing confidentiality, integrity, availability and resilience of Supplier's systems and services;

(ix) maintain and annually test a comprehensive business continuation plan for restoring any of its critical business functions and systems that Process Thomson Reuters Data;

(x) restore the availability and access to Thomson Reuters Data in a timely manner in the event of a physical or technical incident;

(xi) maintain a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing of Thomson Reuters Data, regularly testing such measures to validate their appropriateness and effectiveness, and implementing corrective action where deficiencies are revealed by such testing;

(xii) log all individuals' access to and activities on systems and at facilities containing Thomson Reuters Data. Upon Thomson Reuters' request, Supplier will provide a report detailing a list of authorized users, their associated privileges, status of accounts, and history of activities;

(xiii) for passwords applicable to Supplier's access, adhere to password policies for standard and privileged accounts consistent with industry best practices;

(xiv) protect both Supplier and Thomson Reuters user accounts with access to Thomson Reuters Data using multi-factor authentication (e.g. using at least two different factors to authenticate such as a password and a security token or certificate);

(xv) store and transmit Thomson Reuters Data using strong cryptography, consistent with industry best practices, and pseudonymize Personal Information where appropriate;

(xvi) if connection is permitted by Thomson Reuters, only connect to Thomson Reuters' networks via Virtual Private Network (VPN), without split tunneling, and utilizing strong cryptography consistent with industry best practices;

(xvii) except as otherwise agreed herein, allow Thomson Reuters Data to be removed from Supplier's premises or downloaded to any device only if the Thomson Reuters Data is encrypted using strong cryptography, consistent with industry best practices;

(xviii) ensure that only those Supplier personnel who need to have access to Thomson Reuters Data are granted access, such access is limited to the least amount required, and only granted for the purposes of performing obligations under this Agreement, an Order, or governing agreement referenced by an Order. Supplier shall conduct access reviews upon each individual's scope of responsibility change, Supplier staffing change or other change impacting Supplier personnel access to Thomson Reuters Data;

(xix) maintain a separation of duties to prevent unauthorized tasks or actions from being conducted by unauthorized individuals, including preventing end to end control of a Process by only one individual;

(xx) maintain a physical security program that is consistent with industry best practices (including Section 11 of ISO 27002, as it may change from time to time);

(xxi) segregate (at least logically and if possible, physically) Thomson Reuters Data from other customers' data. Supplier shall notify Thomson Reuters if it cannot physically segregate Thomson Reuters Data;

(xxii) ensure that any storage media (whether magnetic, optical, non-volatile solid state, paper, or otherwise capable of retaining information) that captures Thomson Reuters Data is securely erased or destroyed before repurposing or disposal; and

(xxiii) maintain an employee termination process, which must specify timeframes (which must be prompt and within a reasonable time of any termination) for termination of logical and physical access, including procedures for Supplier to collect any devices or equipment containing Thomson Reuters Data from the terminating employee, prior to termination.

**4. <u>Data Privacy.</u>**

4.1. The parties shall set forth the scope, nature, purpose, duration and other details of the Processing carried out by Supplier in the applicable Order.

4.2. Supplier shall provide reasonable assistance to Thomson Reuters to allow it to conduct privacy impact assessments and to respond to requests from individuals exercising their rights under Data Protection Laws.

4.3. Where Personal Information is located within, or originates from, the European Union (EU) or European Economic Area (EEA), or the United Kingdom (UK), Supplier may not transfer any such Personal Information to any country or territory outside the EEA or the UK (as the case may be), unless either:

4.3.1. it first notifies Thomson Reuters of such transfer, and takes such measures as Thomson Reuters may reasonably specify to ensure such transfer complies with Data Protection Laws, including, at the request of Thomson Reuters, entering into (or procuring that such other third parties as Thomson Reuters may reasonably specify enter into) standard contractual clauses with Thomson Reuters (or such other third party as Thomson Reuters may reasonably specify) provided that: (i) if Supplier Processes Personal Information in a country that has not received an adequacy determination from the EU Commission and such Personal Information pertains to Data Subjects located in the EU or EEA, then the parties agree that the EU/EEA Standard Contractual Clauses apply and are incorporated by this reference; or (ii) if Supplier Processes Personal Information in a country that has not received an adequacy determination from the UK and such Personal Information pertains to Data Subjects located in the UK, then the parties agree that the UK Standard Contractual Clauses apply and are incorporated herein by this reference. For the purposes of this Section 4.3.1 and pursuant to Section 4.1, Thomson Reuters hereby grants consent to the transfers expressly described in any Order signed by both parties; or

4.3.2. transfers are subject to BCR. If transferring Personal Information pursuant to BCR, Supplier warrants and represents that its BCR are approved in all European jurisdictions from which the Personal Information originates. Supplier shall ensure that it, and any of its Affiliates Processing Personal Information from time to time, remains validly bound by such BCR for the duration of such Processing, even if it extends beyond the term of this Agreement or an Order.

Supplier shall promptly provide Thomson Reuters with all cooperation and information reasonably requested by Thomson Reuters in order to determine the applicability of the BCRs to all or part of the Personal Information and the adequacy of BCR as a data protection and transfer mechanism. If the validity of the BCR (or the validity of binding corporate rules more generally as a data transfer mechanism) is challenged by a regulator or in a court, or if the BCR ceases to be recognized as providing adequate protection under the Directive, Supplier shall promptly notify Thomson Reuters and comply with an alternative data transfer mechanism of Thomson Reuters' choosing that provides adequate protection either under the Directive, or pursuant to an adequacy finding by the Commission.

4.4. Where Personal Information is located in a non-EU, non-EEA, or non-UK country or territory that has enacted Data Protection Law(s) restricting transfers of or access to Personal Information, Supplier may not transfer any Personal Information to any other country or territory without the prior written consent of Thomson Reuters. Supplier shall cooperate with Thomson Reuters to execute any agreements and to implement all processes and measures that Thomson Reuters deems appropriate to comply with such country's Data Protection Law(s).

4.5. Where applicable to the services provided, Supplier shall ensure that, in accordance with applicable law and/or Thomson Reuters policies and procedures, all Personal Information Processed on behalf of Thomson Reuters by Supplier shall originate from individuals and entities (including without limitation consumers, business customers and/or Thomson Reuters employees and contractors) who Supplier has properly notified and who have provided appropriate consent to the collection, access, use, maintenance and/or disclosure of the Personal Information. Unless otherwise agreed in writing by Thomson Reuters and Supplier, the appropriate type of consent shall be express ("opt-in") consent.

4.6. Supplier shall obtain prior written consent from Thomson Reuters before transferring Thomson Reuters Data to any sub-processors, and if Thomson Reuters allows such transfer, require such sub-processors to enter into a written contract with Supplier which imposes obligations equivalent to Supplier's obligations with respect to Thomson Reuters Data (including as set out in this Agreement, an Order, or a governing agreement referenced by an Order). Supplier shall ensure the sub-processor complies with such obligations (including by auditing or otherwise taking steps in accordance with good industry practice to confirm such compliance at least annually). Upon request from Thomson Reuters, Supplier shall confirm the timing, scope and findings of any such audit or confirmation exercise. Thomson Reuters hereby grants consent to the sub-processors listed in any Order signed by both parties, subject to compliance with this Section 4.6.

4.7. The parties shall, and Supplier shall ensure that each of the sub-processors shall, comply at all times with the Data Protection Laws and shall not perform their obligations under this Agreement in such a way as to cause either party to breach any of its obligations under any applicable Data Protection Laws. Supplier shall reasonably assist Thomson Reuters to comply with its obligations under Data Protection Laws and shall inform Thomson Reuters if, in Supplier's opinion, Thomson Reuters' instructions would be in breach of Data Protection Laws. On an annual basis and upon request from Thomson Reuters, Supplier shall certify and provide evidence of its and its sub-processors' compliance

with the provisions of this Agreement, including certifying that it is not aware of any facts or events which would jeopardize its status as a Processor under Data Protection Laws.

4.8. Supplier consents to Thomson Reuters disclosing the existence and nature of this relationship as required by Data Protection Laws.

4.9. Supplier shall: (i) promptly (within five days) notify Thomson Reuters if Supplier, its Affiliates, or any sub-processor receives a Data Subject Request or a notification or complaint from a regulatory agency with respect to Thomson Reuters Data or the activities under this Agreement; (ii) not honor or effectuate a Data Subject Request without Thomson Reuters' prior written consent (which shall not unreasonably be withheld); (iii) not directly respond to any Data Subject Request or notification or complaint from a regulatory agency, except upon the written instructions of Thomson Reuters, or as required by the Data Protection Laws; and (iv) promptly cooperate with Thomson Reuters with respect to any Data Subject Request or notification or complaint from a regulatory agency, including without limitation, providing all reasonably requested information or effectuating any Data Subject Request passed through from Thomson Reuters to Supplier, its Affiliates, or any sub-processor with respect to Thomson Reuters Data.

## 5. Audit Rights and Breach Notification.

5.1. In addition to Thomson Reuters' audit rights under an Order or a governing agreement referenced by an Order, Supplier shall, at Thomson Reuters' request, permit Thomson Reuters or its external advisers, and regulators of Thomson Reuters or its customers (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit Supplier's Processing activities and those of Supplier's agents, Affiliates and sub-processors, to verify that Supplier is in compliance with its obligations under this Agreement. The following provisions additionally apply to such audits:

5.1.1. Except in the case of urgency (including a request from a regulator, or an actual or suspected security breach, data loss or misappropriation of Thomson Reuters Data) and unless it would seriously hamper the purpose of the audit, Thomson Reuters shall use reasonable endeavors to give Supplier at least two business days' notice of when the audit will be conducted and an estimate of the audit's duration.

5.1.2. Supplier shall provide all reasonable assistance to, and co-operate with, the auditor. Supplier shall provide copies of all relevant information and reasonable access to premises, personnel, and relevant systems, to the extent (i) allowable by law or (ii) Supplier's third party audited security related reports do not fully allow Thomson Reuters to assess Supplier's compliance with its obligations under this Agreement, in Thomson Reuters' reasonable judgment.

5.1.3. Each party shall bear its own costs of audit, except where the auditor finds that Supplier has materially breached this Agreement, in which case Supplier shall bear all costs of the audit.

5.1.4. If the audit reveals material non-compliance with this Agreement, Thomson Reuters may exercise its termination for cause options under an Order or a governing agreement referenced by an Order.

5.2. Supplier shall immediately notify Thomson Reuters, by emailing privacy.enquiries@thomsonreuters.com, if it becomes aware of, or reasonably suspects, (i) any breach of Data Protection Laws by Supplier or any of its sub-processors in connection with this Agreement; (ii) any breach of this Agreement; or (iii) any unusual activity that represents an actual or potential security threat or security breach on devices or systems hosting Thomson Reuters Data or otherwise being used to deliver services. If any of the foregoing events occur, Supplier shall conduct a thorough investigation of such incident, document the steps for any needed remediation, provide the results of its analysis to Thomson Reuters promptly following the investigation, and implement the needed remediation on the timescales specified by Thomson Reuters.

5.3. Supplier shall assign one or more Supplier personnel, and communicate to Thomson Reuters the name(s) of such Supplier personnel, to manage security breach communications. In the event of a breach, such Supplier personnel will be available to Thomson Reuters 24 hours a day, 365 days a year, to facilitate and respond to issues related to this Agreement.

5.4. Subject to the terms and conditions of the applicable Order and any governing agreement referenced by an Order, Supplier shall bear all costs that Thomson Reuters incurs related to a security breach or data protection incident arising from or related to Supplier's breach of its obligations under this Agreement including without limitation: costs to conduct an investigation, cost to notify consumers and others required by law or Thomson Reuters policy, and all fines and penalties.

**6. Term and Termination.**

6.1. **Agreement Term.** This Agreement is effective for seven years from the Effective Date (the "Initial Term"). After the Initial Term, this Agreement automatically renews for consecutive one-year terms (“Renewal Term(s)”).

6.2. **Agreement Termination Without Cause.** Either party may terminate this Agreement upon 30 days' written notice to the other party prior to the commencement of any Renewal Term. Notwithstanding the foregoing, this Agreement continues to govern any Order outstanding at the time of termination as if it had not been terminated.

**7. Assignment.** Except as permitted under this Agreement, neither party may assign its rights or obligations under this Agreement without the other’s prior written consent, which consent may not be unreasonably withheld. However, prior written consent is not required if Thomson Reuters assigns this Agreement, or portion thereof, to one of its Affiliates or to a third party successor-in-interest. This Agreement is binding upon the parties’ respective successors and permitted assigns.

**8. Governing Law and Venue.** The jurisdictional venue and the laws of the state, province, or country specified in an Order or a governing agreement referenced by the Order, govern this Agreement.

**9. Notices.** Details for notices and other communications shall be as provided in the Order or a governing agreement referenced by an Order.

**10. Severability.** If a court or regulatory agency with proper jurisdiction determines that a provision of this Agreement is invalid, then that provision will be interpreted in a way that is valid under applicable law or regulation. If any provision is invalid, the rest of this Agreement will remain effective.

**11. Conflicts.** In the event of any conflict between the terms and conditions set forth in this Agreement and any Order agreed upon by the parties, the terms and conditions of such Order, including any exhibits or attachments thereto, prevail so long as they reference the provisions of this Agreement with which they are inconsistent. Any preprinted terms on Thomson Reuters’ purchase order or on Supplier's quotation, acknowledgment, invoice, click-wrap license, shrink-wrap license or similar documents which conflict with this Agreement are deemed superseded by this Agreement.

**12. Counterparts.** This Agreement may be signed in one or more counterparts and each counterpart will be considered an original. All of the counterparts will be considered one document. Each party may sign and deliver this Agreement by e-mail or other electronic means.

**13. Entire Agreement.** The documents referenced by this Agreement are integral parts of this Agreement and are fully incorporated herein by this reference. This Agreement is the entire agreement between the parties and supersedes all previous agreements, written or oral, between the parties with respect to this Agreement’s subject matter and cannot be modified except in a writing signed by the parties.

By signing below, each party represents that it has read this Agreement, understands it, and agrees to be bound by it.

**THOMSON REUTERS HOLDINGS INC.**

By: _____

Name: _____

Title: _____

Date: _____

**Supplier:**

**Address:**

**City:**

**State:**

**Postal Code:**

**Country:**

By: _____

Name: _____

Title: _____

Date: _____