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 SupplierName, a <State_____> <Entity Type _____> with offices at Address1, City, State, PostalCode ("Company"). 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 Company (or any Company 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 Company 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 Company, 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 Company. Thomson Reuters Data includes Personal Information and Sensitive Personal Information.

2. General. Unless otherwise agreed by Thomson Reuters and Company, all Thomson Reuters Data is and shall remain the exclusive property of Thomson Reuters. Company 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.

Company 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.

Company 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, Company shall return any Thomson Reuters Data under Company'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.

Company 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. Company 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 III 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 Company'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 Company'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, Company 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 Company's access, adhere to password policies for standard and privileged accounts consistent with industry best practices;

(xiv) protect both Company 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 Company'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 Company 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. Company shall conduct access reviews upon each individual's scope of responsibility change, Company staffing change or other change impacting Company 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. Company 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 Company to collect any devices or equipment containing Thomson Reuters Data from the terminating employee, prior to termination.

4. Data Privacy.

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

4.2. Company 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), Company may not transfer any such Personal Information to any country or territory outside the EEA 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) in the form approved by the EU Commission, incorporated by reference as Attachment 1. 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, Company warrants and represents that its BCR are approved in all European jurisdictions from which the Personal Information originates. Company 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.

Company 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, Company 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 or non-EEA country or territory that has enacted Data Protection Law(s) restricting transfers of or access to Personal Information, Company may not transfer any Personal Information to any other country or territory without the prior written consent of Thomson Reuters. Company 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, Company 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 Company shall originate from individuals and entities (including without limitation consumers, business customers and/or Thomson Reuters employees and contractors) who Company 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 Company, the appropriate type of consent shall be express ("opt-in") consent.

4.6. Company 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 Company which imposes obligations equivalent to Company'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). Company 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, Company 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 Company 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. Company shall reasonably assist Thomson Reuters to comply with its obligations under Data Protection Laws and shall inform Thomson Reuters if, in Company's opinion, Thomson Reuters' instructions would be in breach of Data Protection Laws. On an annual basis and upon request from Thomson Reuters, Company 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. Company consents to Thomson Reuters disclosing the existence and nature of this relationship as required by Data Protection Laws.

4.9. Company shall: (i) promptly (within five days) notify Thomson Reuters if Company, 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 Company, 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, Company 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 Company's Processing activities and those of Company's agents, Affiliates and sub-processors, to verify that Company 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 Company at least two business days' notice of when the audit will be conducted and an estimate of the audit's duration.

5.1.2. Company shall provide all reasonable assistance to, and co-operate with, the auditor. Company 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) Company's third party audited security related reports do not fully allow Thomson Reuters to assess Company'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 Company has materially breached this Agreement, in which case Company 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. Company 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 Company 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, Company 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. Company shall assign one or more Company personnel, and communicate to Thomson Reuters the name(s) of such Company personnel, to manage security breach communications. In the event of a breach, such Company 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, Company shall bear all costs that Thomson Reuters incurs related to a security breach or data protection incident arising from or related to Company'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 Company'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: _____

<COMPANY>

By: _____

Name: _____

Title: _____

Date: _____

Attachment 1

to the
Data Protection Agreement

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, Thomson Reuters (as data exporter) and Company (as data importer), each a 'party'; together 'the parties',

have agreed on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the party who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

(a) The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

(b) The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

(c) The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

(d) The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

(e) These Clauses are agreed for the benefit of the data exporter and for all members of the data exporter's corporate group (including Thomson Reuters Group Limited and any entity that, from time to time, directly or indirectly controls, is controlled by, or is under common control with Thomson Reuters Group Limited, or that is a successor to any such entity or its business and assets), and each such member may enforce and rely on these Clauses to the same extent as if it was a party to these Clauses and had the same rights as the data exporter.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) that in the event that the European Commission, the European Court of Justice, the Article 29 Working Party, or any supervisory or other relevant authority determines that these Clauses do not (or no longer) provide a valid basis for such processing or transfer, the data importer shall promptly put in place any measures reasonably requested by the data exporter in order to ensure continued compliance with Clause 4(a);

(g) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of

independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(h) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(i) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(j) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(k) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

(a) The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

(b) If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

(c) The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

(d) If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

(a) The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(i) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(ii) to refer the dispute to the courts in the Member State in which the data exporter is established.

(b) The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

(a) The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

(b) The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

(c) The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of England and Wales.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

(a) The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

(b) The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

(c) The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

(d) The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

(a) The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

(b) The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter: Thomson Reuters

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any): (stamp of organisation)

Signature .....

On behalf of the data importer: Company

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any): (stamp of organisation)

Signature .....

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses. The data exporter, data importer, data subjects, categories of data, special categories of data, and processing operations are defined in the Order.

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

The description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached) is included within the Agreement.