Thomson Reuters™

THOMSON REUTERS SUPPLY CHAIN DATA PROCESSING ADDENDUM

This **SUPPLY CHAIN DATA PROCESSING ADDENDUM** (“***DPA***”) is entered into between Thomson Reuters and Supplier pursuant to any underlying agreement, between Thomson Reuters and Supplier for the provision of Solutions and that references and incorporates this DPA (referred to herein in the singular, “***Agreement***”). This DPA sets out Supplier’s obligations with respect to the Processing of Thomson Reuters Data by Supplier pursuant to the Agreement. Capitalized terms used in this DPA shall have the meanings attributed to them as set forth in ***Section 6 (Definitions & Interpretation)***.

1. PROCESSING OF THOMSON REUTERS DATA AND SUPPLIER’S ROLE.

1.1. **Compliance with Laws; Compliance Program.** Supplier shall, at all times, comply with all Applicable Laws when Processing Thomson Reuters Data, including the portions of those Applicable Laws governing Processors. Supplier represents, warrants, and covenants that it will conduct regular risk assessments and implement and maintain a comprehensive data protection program (governing data privacy and data security) to meet its obligations under Applicable Laws and this DPA, and mitigate any threats or risks identified by Supplier.

1.2. **Role & Cooperation.** With respect to the Processing of Thomson Reuters Data, the parties agree that: (a) Thomson Reuters is the Controller, and Supplier is the Processor, subject to Section 4 (Controller to Controller); (b) the details of the processing activities by Supplier are outlined in the Agreement; and (c) Supplier shall: (i) inform Thomson Reuters if an instruction violates any Applicable Laws; (ii) provide assistance and relevant information for Thomson Reuters to meet its legal obligations; and (iii) stop processing and inform Thomson Reuters if it cannot meet any obligation under the Agreement (including this DPA) or Applicable Law.

2. OBLIGATIONS OF SUPPLIER.

2.1. **Limitations on Processing.** Supplier shall Process Thomson Reuters Data only in strict accordance with Thomson Reuters’s written instructions, including those expressly set forth in the Agreement.

> 2.1.1. **Specific Prohibitions.** Without limiting the generality of the foregoing, and unless Supplier has obtained prior express written consent from Thomson Reuters, Supplier shall not: (a) retain, use, exploit, Sell, disclose, or otherwise Process Thomson Reuters Data, whether or not anonymized, for any other purpose; (b) attempt to or actually re-identify (or re-associate to a Data Subject) any anonymized, de-identified, or pseudonymized data provided by Thomson Reuters; (c) combine Thomson Reuters Data with data received from another source or with data collected by Supplier from its own interactions with Thomson Reuters’s consumers (e.g., employees, users, etc.); (d) use or otherwise Process Thomson Reuters Data, including any data or information derived from Thomson Reuters Data, to develop, test, train, or improve any algorithm or artificial intelligence or machine learning (“***AI/ML***”) model; or (e) make automated decisions affecting Data Subjects or make decisions affecting Data Subjects based on the profiling of such individuals.

2.2. **Direct Collection of Data.** If, pursuant to the Agreement, Supplier collects Personal Data directly from or generates Personal Data about a Data Subject(s), Supplier shall: (a) only collect or generate the minimum amount and types of Personal Data necessary to provide its Solutions; (b) obtain and record, and make available if requested, all necessary consents from and/or provide all necessary notices to such Data Subject(s) as required by Applicable Laws to enable Supplier to lawfully, fairly, and transparently Process such Personal Data; and (c) upon request, promptly provide Thomson Reuters evidence of each Data Subject's consent and/or the notices provided to each Data Subject.

2.2.1. **Digital Advertising.** If, pursuant to the Agreement, Supplier provides any Solutions related to Digital Advertising, then the terms set forth in the ***Digital Advertising Addendum*** attached hereto and incorporated herein as ***Exhibit B*** shall apply.

2.3. **Personnel.** Supplier shall ensure it and its personnel (including staff, agents, and Subprocessors) who handle Thomson Reuters Data are subject to a duty of confidentiality and treat Thomson Reuters Data as the proprietary and confidential information of Thomson Reuters in accordance with Supplier's obligations in the Agreement (including this DPA).

2.4. **Security.** Supplier shall implement and maintain all appropriate physical, technical, and organisational safeguards to: (a) ensure the security and confidentiality of Thomson Reuters Data and the systems used to Process it; (b) protect against any threats or hazards to the security or integrity of Thomson Reuters Data and systems used to Process it; and (c) protect Thomson Reuters Data against unauthorized destruction, loss, alteration, use, disclosure, or access. The parties agree that the specific safeguards maintained and implemented by Supplier shall, at a minimum, include those measures set forth in the ***Supply Chain Data Security Addendum*** attached hereto as ***Exhibit A*** (the "***DSA***").

2.5. **Access Requests.** Supplier shall promptly (within five business days) provide all information and assistance to enable Thomson Reuters to fulfill a Data Subject Rights Request related to Supplier's Processing of Thomson Reuters Data, including to effectuate any Data Subject Rights Request passed from Thomson Reuters to Supplier. If Supplier receives a Data Subject Rights Request directly from a Data Subject or a request, correspondence, inquiry, or complaint from law enforcement or another governmental agency related to Thomson Reuters Data, it will promptly (within no more than five business days) refer the same to Thomson Reuters (to the extent permissible) for handling and Supplier shall not directly respond to the Data Subject or law enforcement or another governmental agency (unless legally required to do so) without prior written approval from Thomson Reuters.

2.6. **Deletion and Retention.** Throughout the course of the Agreement, Supplier shall retain each dataset (comprising the Thomson Reuters Data) only for the minimum period necessary for Supplier to provide its Solutions; and, thereafter, securely return or delete, at Thomson Reuters's election, such Thomson Reuters Data (even if the Agreement has not yet terminated).

Furthermore, upon request and upon the expiration or termination (for any reason) of the Agreement or an applicable Order, Supplier shall securely return or delete (at Thomson Reuters's election) all Thomson Reuters Data in its or its Subprocessors' possession. Upon request, Supplier shall promptly deliver to Thomson Reuters written confirmation signed by an authorized representative of Supplier that it has returned or deleted such data in accordance with this Section.

2.6.1. **Record Retention Compliance.** Notwithstanding the foregoing, Supplier may retain one copy of any subset of Thomson Reuters Data to the extent required by Applicable Law, provided that Supplier shall: (a) inform Thomson Reuters of its requirement to retain such data and the required retention period thereof; (b) delete all other Thomson Reuters Data from the dataset (so that only the subset of Thomson Reuters Data required by Applicable Law is retained); (c) isolate and prevent any further active Processing (except to the extent required by Applicable Law) of such data; (d) protect such data in accordance with the terms of the Agreement (including this DPA); and (e) immediately and securely delete such data once the required retention period expires.

2.7. **Subprocessors.** Supplier shall: (a) obtain prior written consent from Thomson Reuters before engaging any Subprocessor, including new or changed Subprocessors; (b) impose data protection terms on any Subprocessor no less protective of Thomson Reuters Data and no less restrictive than the terms of the Agreement (including this DPA); (c) upon request from Thomson Reuters, provide Thomson Reuters a copy of such data protection terms; (d) ensure its Subprocessors' compliance with such data protection terms and Applicable Laws, including by auditing or otherwise taking steps in accordance with standard industry practice to confirm such compliance on an annual basis (and, upon request from Thomson Reuters, Supplier shall confirm the timing, scope, and findings of any such audit or confirmation exercise); and (d) remain liable for any acts or omissions of its Subprocessor(s). Thomson Reuters hereby grants consent to the Subprocessors listed in any Order signed by the parties.

2.7.1. **Objection.** If Thomson Reuters does not consent to the use of a new or changed Subprocessor, then Supplier shall provide the Solutions without use of the objectionable Subprocessor or, if that is not reasonably feasible, Thomson Reuters shall have the right to terminate the Agreement without penalty.

2.8. **Audits.** Upon written request from Thomson Reuters, Supplier shall allow and contribute to inspections and audits by Thomson Reuters or an external auditor, subject to the Agreement's confidentiality obligations. Where relevant and agreed upon by Thomson Reuters, Supplier may satisfy this requirement by providing its latest third-party audits or certifications. For inspections of Supplier's systems and premises, the parties will agree on the scope, methodology, timing, and conditions in good faith; provided, however, that, if they cannot agree, Thomson Reuters shall make the final determination taking into account legal requirements, any security incidents or deficiencies, and inquiries from customers or authorities. Each party shall be responsible for its own costs related to an audit or inspection, unless Supplier is found in breach of the Agreement, in which case Supplier shall bear all costs. Supplier shall promptly remediate any deficiencies found as part of an audit or inspection and, where applicable, in accordance with the timelines set forth in Section 2.5 of the DSA.

3. DATA TRANSFERS.

3.1. **Transfer Requirements**. Supplier shall obtain prior written consent from Thomson Reuters before Transferring (including any onward Transfers of) any Thomson Reuters Data to a new jurisdiction. Notwithstanding any such consent by Thomson Reuters, Supplier shall only transfer Thomson Reuters Data when and as permitted by Applicable Law. Without limiting the foregoing, the parties agree that:

3.1.1. **Transfers of European Personal Data.** To the extent Thomson Reuters and/or Supplier participate in a Data Privacy Framework (DPF) and such party's participation governs the relevant Transfer of Personal Data, then Supplier shall comply with all requirements of the Data Privacy Framework, including the DPF Principles. If European Data Protection Laws require that appropriate safeguards are put in place (for example, if the Data Privacy Framework does not cover the relevant Transfer to Supplier and/or the relevant DPF is invalidated), the following Standard Contractual Clauses will be incorporated by reference and form part of the Agreement as follows: Without limiting the foregoing, the parties agree that the terms of the GDPR Standard Contractual Clauses[1] and, as appropriate, the UK International Data Transfer Addendum to the SCCs[2] or the UK International Data Transfer Agreement[3] shall apply to any Transfers of Personal Data governed by GDPR (or by the Applicable Laws of a jurisdiction other than the EU/EEA where such laws expressly recognize the GDPR Standard Contractual Clauses as a mechanism to legitimize the Transfer of Personal Data) and/or the UK GDPR, respectively, to a country that has not received an adequacy decision, provided that, where required by Applicable Law, Supplier shall first perform a Transfer Impact Assessment and implement any required additional safeguards prior to receiving the Personal Data.

3.1.2. **Transfers of Non-European Personal Data.** If any other Applicable Law requires the participation of Thomson Reuters to legitimize the Transfer of Personal Data, such as the collection of consent from Data Subjects or the execution of Standard Contractual Clauses, then Supplier shall notify Thomson Reuters and the parties will cooperate in good faith to implement the required transfer mechanism prior to Transferring the Personal Data.

4. CONTROLLER TO CONTROLLER TERMS. Where the parties have agreed in an applicable Order that Supplier acts as a Controller with respect to specific Personal Data, the parties agree that (a) each party acts as a separate, independent Controller to one another and that the Agreement (including this DPA) is not intended to establish a joint Controller relationship and

[1] Link: https://www.thomsonreuters.com/content/dam/ewp-m/documents/thomsonreuters/en/pdf/global-sourcing-procurement/eu-eea-standard-contractual-clauses-v12-2021.pdf
[2] Link: https://www.thomsonreuters.com/content/dam/ewp-m/documents/thomsonreuters/en/pdf/global-sourcing-procurement/uk-addendum-2022.pdf
[3] Link: https://www.thomsonreuters.com/content/dam/ewp-m/documents/thomsonreuters/en/pdf/global-sourcing-procurement/uk-international-data-transfer-agreement-2022.pdf

(b) the terms and conditions of this section, in addition to the remainder of this DPA (and all terms and conditions of the Agreement), shall apply to Supplier and its Processing of Thomson Reuters Data in its role as a Controller. The parties shall expressly set forth in the applicable Order the categories of Personal Data and the relevant Data Subjects where Supplier acts as a Controller thereof, as well as the specific Processing activities to be performed by Supplier in its role as a Controller. In addition to the other terms of the Agreement and this DPA, Supplier agrees that it is fully responsible and solely liable under Applicable Laws with respect to its Processing of such Personal Data as Controller thereof. Without limiting the foregoing, Supplier: (i) shall obtain all necessary consents and provide all necessary notices as required by Applicable Laws for Supplier to lawfully, fairly, and transparently Process such Personal Data as Controller thereof; (ii) contractually covenants, despite its role as a Controller, to (1) only Process the relevant Thomson Reuters Data for the specific Processing activities outlined in the applicable Order and (2) comply with the limitations set forth in Subsection 2.1.1; and (iii) notwithstanding anything to the contrary in ***Section 2.5 (Access Requests)***, shall be responsible for directly responding to and/or fulfilling all Data Subject Rights Request or a request, correspondence, inquiry, or complaint from a law enforcement or another governmental agency that relates to its Processing of such Personal Data as Controller thereof. Unless otherwise agreed in writing by Thomson Reuters, when Processing Sensitive Personal Data and whenever else required by Applicable Law, Supplier covenants, despite its role as a Controller, to collect prior affirmative ('opt-in') consent.

5. GENERAL. All other terms and conditions of the Agreement remain in full force and effect. Unless otherwise agreed in writing in the Agreement, all Thomson Reuters Data is and shall remain the exclusive property of Thomson Reuters. Any breach of this DPA (including the DSA) shall be deemed a material breach of the Agreement. For any inconsistencies between this DPA and the Agreement, this DPA shall prevail as it relates to the Processing of Thomson Reuters Data only, provided that the Agreement will prevail if it expressly identifies the terms of this DPA to be superseded. For any inconsistencies between this DPA and an Applicable Law for a specific jurisdiction, the Applicable Law for that specific jurisdiction shall prevail only as it relates to the Processing activities governed by that specific jurisdiction's Applicable Law.

6. DEFINITIONS & INTERPRETATION

6.1. "***Applicable Law***" means any law or regulation, including any data privacy and cybersecurity law, to the extent applicable to a party's Processing of Thomson Reuters Data. Applicable Law includes applicable data privacy and cybersecurity law of the jurisdiction where Supplier's Processing activities actually occur, as well as that of the jurisdiction where the Personal Data originated or where the Data Subject is located.

6.2. "***Controller***" (also referred to as "***Business***" or "***Operator***" under certain Applicable Laws) means the natural person or legal entity, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

6.3. “***Data Privacy Framework***” or “***DPF***” means the Transfer mechanisms developed by the U.S. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration to provide U.S. organizations with reliable mechanisms for Personal Data Transfers to the United States from the European Union, United Kingdom, and Switzerland while ensuring data protection consistent with EU, UK, and Swiss law. DPF includes (a) the EU-U.S. DPF, (b) the UK Extension to the EU-U.S. DPF, and (c) the Swiss-U.S. DPF.

6.4. “***Digital Advertising***” means marketing or other advertisements that are served, presented, or otherwise delivered to a Data Subject on a digital property (such as a website or mobile application). Digital Advertising includes (a) advertising delivered to a Data Subject based solely on the content of the digital property where the advertisement is served, the context of the Data Subject’s current visit, or information available in real time about the Data Subject’s network or device (“***Contextual Ads***”) and (b) targeting of advertising to Data Subject based on their Personal Data, including Personal Data obtained from their online activity across numerous digital properties (sometimes referred to as “targeted advertising”, “interest-based advertising”, or “cross-context behavioral advertising”).

6.5. “***DPF Principles***” means the binding set of requirements that govern DPF-participating organizations’ use and treatment of Personal Data received from the EU/UK or Switzerland under, respectively, the EU-U.S. Data Privacy Framework Principles (which apply to the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF) and the Swiss-U.S. Data Privacy Framework Principles (which apply to the Swiss-U.S. DPF). The DPF Principles include the binding requirements set forth here.

6.6. “***Data Subject***” (also referred to as “***Consumer***” under certain Applicable Laws) means the natural person to whom the Personal Data pertains.

6.7. “***Data Subject Rights Request***” means a request from a Data Subject to exercise a right afforded to them under an Applicable Law or by Thomson Reuters with respect to the control or use of, or disclosures relating to, their Personal Data (including the right to access, correct, delete, or require an entity to stop the Processing of their Personal Data).

6.8. “***Personal Data***” (also referred to as “***Personal Information***” or “***Personally Identifiable Information***” under certain Applicable Laws) means any information relating to an identified or identifiable natural person, in which 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 Data includes information that could reasonably be linked, directly or indirectly, or inferred with a particular individual or household.

6.9. “***Process***” means any operation or set of operations performed upon data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, Transfer, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

6.10. “***Processor***” (also referred to as “***Service Provider***” or “***Entrusted Party***” under certain Applicable Laws) means the natural person or legal entity, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

6.11. “***Security Incident***” means, collectively: (a) the reasonably suspected or actual unauthorized access, use, disclosure, modification, loss, or destruction of Thomson Reuters Data, whether originating with Supplier, its affiliate, or its Subprocessor; (b) any breach of Applicable Laws by Supplier or any of its Subprocessors as it relates to data protection (including data security and privacy); (ii) any breach of this DPA or the DSA. For clarity, a Security Incident includes, but is not limited to: a ‘personal data breach’ as that term is defined under GDPR; ‘breach of system security’ (or analogous term) under U.S. state data breach notification laws; or similar terms under Applicable Laws.

6.12. “***Sell***” or “***Selling***” means selling, renting, releasing, disclosing, disseminating, making available, Transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject’s Personal Data to another party for monetary or other valuable consideration.

6.13. “***Sensitive Personal Data***” is a subset of Personal Data and means any Personal Data that requires additional or enhanced protection under Applicable Laws as a result of its sensitive nature. Examples of Sensitive Personal Data include ‘special categories of data’ under the General Data Protection Regulation (“***GDPR***”), ‘protected health information’ under the Health Insurance Portability and Accountability Act of 1996 (“***HIPAA***”), ‘biometric under the Illinois Biometric Information Privacy Act (“***BIPA***”), 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).

6.14. “***Share***” or “***Sharing***” means the sharing, disclosing, transferring, distributing, copying, or otherwise making available of Personal Data in connection with Digital Advertising.

6.15. “***Solutions***” means the products or services provided by Supplier to Thomson Reuters pursuant to the Agreement.

6.16. “***Standard Contractual Clauses***” means those model clauses approved pursuant to Applicable Law that legitimize the Transfer of Personal Data across borders, including, for example, the Standard Contractual Clauses approved pursuant to GDPR by the European Commission (“***GDPR Standard Contractual Clauses***”).

6.17. “***Subprocessor***” means any subcontractor, including an affiliate of Supplier, providing products or services where such subcontractor Processes any Thomson Reuters Data.

6.18. “***Supplier***” means the legal entity which has directly entered into the Agreement with Thomson Reuters, including any of its affiliates.

6.19. “***Thomson Reuters***” means the named Thomson Reuters entity that has entered into the Agreement for Solutions with Supplier and any affiliate Thomson Reuters entities to whom the Agreement may apply.

6.20. “***Thomson Reuters Data***” means all data or information, including Personal Data, Metadata, and derivatives of such data or information, that is either (i) submitted or made available by or on behalf of Thomson Reuters (including its agents, customers, suppliers, contractors, and outsourcers) to Supplier or (ii) generated by Supplier in the course of providing its Solutions to Thomson Reuters. For purposes of this definition and DPA, “***Metadata***” means any data that describes or provides information pertaining to Thomson Reuters (including its agents, customers, suppliers, contractors, and outsourcers), its Data Subjects, or Thomson Reuters Data, including, but not limited to, traffic data, transmission data, and tracking data.

6.21. “***Transfer***” means the sharing, disclosing, transferring, distributing, copying, or otherwise making available of Thomson Reuters Data across geographic borders. Transfers include providing remote electronic access to an individual or entity located in a different jurisdiction, even if the data physically remains on servers located in the original jurisdiction.

6.22. **Interpretation**. Unless otherwise defined in this DPA (including the DSA), any capitalized terms used have the meanings ascribed to them in the Agreement. The words “include”, “includes”, and “including” as used herein shall not be construed to be limiting, but instead be deemed to be followed by the words “without limitation”. The section headings in this DPA are for convenience only and shall not be used for interpretive purposes. The word “or” as used herein is not exclusive and is deemed to have the meaning “and/or”. References in this DPA to any agreement, instrument, or other document mean such agreement, instrument, or other document as amended, supplemented, and modified from time to time to the extent permitted by the Agreement. No provision, uncertainty or ambiguity in or with respect to this DPA shall be construed or resolved against any party hereto, whether under any rule of construction or otherwise. On the contrary, this DPA has been reviewed by each of the parties hereto and shall be construed and interpreted according to the ordinary meaning of the words used so as to fairly accomplish the purposes and intentions of the parties.

EXHIBIT A: SUPPLY CHAIN DATA SECURITY ADDENDUM (DSA)

1. INFORMATION SECURITY PROGRAM

1.1 Supplier shall maintain an information security program that adopts the International Organization for Standardization (ISO/IEC 27002:2013) and/or the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The program must include, but is not limited to, the following components:

(i) Information security policy framework;

(ii) Management direction;

(iii) Program documentation;

(iv) Auditable controls;

(v) Compliance records; and

(vi) Appointed security officer and information security personnel.

1.2 Conduct regular risk assessments periodically (minimum annually) and upon significant organizational, IT or other relevant changes. Supplier must document the risk assessment results and implement corresponding risk treatment plans.

1.3 Comply with requirements of applicable data protection laws and regulations.

1.4 Plan and train (no less than annually) all employees and contractors regarding defined information security policies, standards and customers' security requirements.

2. DATA SECURITY CONTROLS. Supplier shall establish and maintain adequate data security controls (including those listed below) to protect all Thomson Reuters Data in the control or possession of Supplier or its affiliates or Subprocessors against accidental, unauthorized, or unlawful Processing and against accidental loss, destruction, damage, alteration, disclosure, or access.

2.1 **User Access Management.** To protect the confidentiality and integrity of Thomson Reuters Data, Supplier must maintain a robust user access management program aligned to International Organization for Standardization (ISO/IEC 27002:2013), which includes:

(i) Implementing formal, documented access control policies to support provisioning and deprovisioning of user accounts for systems and applications holding or allowing access to Thomson Reuters Data.

(ii) User account privileges must be allocated on a "least privilege" basis and must be formally authorized and documented.

(iii) Generic, service and "shared" accounts must have system owners assigned and controls enabled to track specific users.

(iv) Conducting quarterly (privileged users) and bi-annually (all other users) access review for all systems and applications have access to Thomson Reuters Data and provide executive summary of the review to Thomson Reuters on request.

(v) Log all individuals' access to systems and facilities containing or Processing Thomson Reuters Data.

(vi) Upon termination or change of employment responsibilities, user access rights to systems and applications storing or allowing access to Thomson Reuters Data must be removed promptly (and, in any event, no later than 24 hours after a termination or one calendar week after a change of responsibilities).

(vii) Multi-factor authentication for systems and application processing Thomson Reuters Data.

2.2 **Application Strategy, Design, and Acquisition.** Deploy security-by-design throughout the entire lifecycle of any Supplier systems that Process or could establish access to Thomson Reuters Data or Thomson Reuters systems, which shall at a minimum include SDLC policies and processes for:

(i) Implementing formal, documented change control procedures to manage changes to information systems, supporting infrastructure, and facilities.

(ii) Logically or physically separating environments for development, testing, and production.

(iii) Restricting and tracking user access to program source code.

(iv) Testing system and application changes against defined acceptance criteria prior to implementation.

(v) Not allowing use of Thomson Reuters production data in a non-production environment. If usage is unavoidable, data must be masked (e.g. obfuscated, sanitized, de-identified, anonymized) or the non-production environment must have security controls equivalent to those required for production environments.

(vi) Source code must undergo automated static source code analysis and vulnerability remediation prior to implementation.

(vii) Post-implementation testing after system changes, to validate that existing applications and security controls were not compromised.

(viii) Testing and validating that any outsourced system development activities comply with Supplier's information security requirements.

2.3 **Anti-Virus and Anti-Malware.** Deploy and maintain anti-virus and anti-malware capabilities, which shall, at a minimum, include the following:

(i) Detecting and preventing malware, malicious code and the unauthorized execution of code. Controls must be updated regularly with the latest technology available (e.g. deploying the latest signatures and definitions).

(ii) Automatically updating all endpoints with the latest signatures and definitions of antivirus and anti-malware software.

2.4 **Network Security.** Supplier must follow NIST SP 800-215 framework for network security, and Supplier shall, at a minimum:

(i) Maintain and periodically review an inventory of network devices such as wireless access points, routers, servers, and other devices.

(ii) Implement firewalls to control access between trust zones.

(iii) Implement network segmentation, for better access control of trust zones.

(iv) Implement Intrusion Detection (IDS)/Intrusion Prevention (IPS) Systems covering ingress/egress traffic.

(v) By policy and/or technical control, prohibit split tunnelling or bridged internet connections while remotely connected to the Thomson Reuters network. Every connection between internal and external entities must be managed by firewall/approved proxy/security gateway and monitored using intrusion detection/prevention devices.

(vi) If connection is permitted by Thomson Reuters, connect to Thomson Reuters's networks only via a Virtual Private Network (VPN) or virtual desktop infrastructure (VDI) as approved by Thomson Reuters (without split tunneling), utilizing strong cryptography consistent with industry best practices.

2.5 **Physical and Environmental Security.** Supplier's Solutions must be housed in secure facilities protected by a secure perimeter, with ISO 27001 standards/ NIST CSF or industry standard security barriers and entry controls for providers of similar services, including:

(i) Such facilities must be a physically segregated, with guards, logged access, measures to prevent direct visibility, and strict visitor registration and escort protocols.

(ii) Installation of security cameras and data centre/equipment room doors. Cameras must not record sensitive information (e.g. data on workstation screens). Cameras must be monitored by authorised personnel and recordings must be retained for at least 30 days.

(iii) Controls to prevent tampering with, and removal of, computing equipment.

(iv) Posting security awareness reminders within the facilities.

(v) Maintaining proper procedures for visitors and guests accessing such facilities.

(vi) Designing physical safeguards to protect Supplier's systems from security threats and environmental hazards.

(vii) At Thomson Reuters's reasonable request, Supplier shall fully cooperate in providing access to Supplier facilities.

2.6 **Vulnerability Management.** Supplier must implement a patch and vulnerability management process to identify, prioritize, remediate, and deploy or exempt the required security patch to secure the overall Information Technology (IT) environment. IT asset manager must identify the relevant security patches (via vendor website, mailing list, approved websites, newsgroups, National Vulnerability Data (NVD), Common Vulnerabilities and Exposures (CVE) database) and keep Supplier assets updated and patched by:

(i) At least monthly scan for all systems and weekly scans for critical assets and high-risk environments. Continuous vulnerability scanning tools that constant monitor for new vulnerabilities must be deployed.

(ii) Performing vulnerability scans on all critical systems and applications for all major system or application upgrades.

(iii) Developing and implementing risk-based procedures for remediating identified vulnerabilities, approved by the system owner, and once a patch or workaround is available, addressing vulnerabilities based on the severity and industry standards.

(iv) Conducting, annually and after significant changes, penetration testing for systems and applications that store or access Thomson Reuters Data, including Personal Data. Upon Thomson Reuters's request, Supplier must provide executive summary of testing results, including scope, methodology, severity findings (critical, high, medium), the third-party tester's name, and the testing date. Any vulnerabilities identified as "Critical" or "High" by Thomson Reuters must be remediated according to the timeline in the DSA.

(v) Performing security testing for common security coding errors and vulnerabilities against systems holding or processing Thomson Reuters Data to identify any security flaws and provide evidence of remediation for such security flaws at Thomson Reuters's request, in line with ISO 27001 standards or NIST security framework or industry standards.

(vi) Remediating "Emergency" and "Critical" (CVSS rating 10-9) vulnerabilities immediately, and "High" vulnerabilities within 30 days, "Medium" vulnerabilities within 90 days, and "Low" vulnerabilities within 180 days.

(vii) Quarterly scanning systems holding or processing Thomson Reuters Data for security vulnerabilities.

(viii) Using only updated and authorized software and refraining from installing any unauthorized software on any systems or devices that process Thomson Reuters Data or connect to Thomson Reuters's network.

(ix) Following ISO 27001 standards or NIST Cybersecurity Framework or industry best practice for security patching process.

2.7 **Cryptographic, Information Exchange and Transfer Controls.** Supplier shall store and transmit Thomson Reuters Data using strong cryptography consistent with ISO 27001 standards or NIST Cybersecurity Framework or industry best practices, which, at a minimum, shall comply with the following:

(i) Supplier must implement industry standard cryptographic key management procedures, such as approved key lengths, secure administration of keys, immediate revocation of keys upon compromise or change in user employment, recovery of lost or expired keys, backup and archive of keys, key activation and deactivation dates, restricted access to keys, etc.

(ii) Keys must be rotated periodically (master keys at least once a year or immediately when a vulnerability renders a master key no longer secure, and encryption keys twice a year or immediately when a vulnerability renders the encryption keys no longer secure).

(iii) Application and storage keys rotation policy must be enforced for every application in production.

(iv) Thomson Reuters Data, including Personal Data, must be encrypted (minimum TLS 1.2 and AES 256) during transmission across networks, including over untrusted networks (e.g. public networks) and when writing to removable devices.

(v) Supplier must use platform and data-appropriate encryption (e.g., AES-256, TLS 1.2) in non-deprecated, open/validated formats and standard algorithms.

2.8 **Termination.** Supplier must comply with a documented termination or conclusion of service process that includes:

(i) Non-disclosure and confidentiality obligations with respect to Thomson Reuters Data, including Personal Data, must remain in place following service agreement termination or conclusion.

(ii) A primary point of contact must be identified to support the service termination process.

(iii) Communicating agreement termination or conclusion to relevant employees and stakeholders.

(iv) Revoking access to systems and applications storing or allowing access to Thomson Reuters Data promptly upon completion or termination of the service agreement.

(v) Returning hardware, software, middleware, documents, data, information and other assets owned or leased from Thomson Reuters.

(vi) Return to Thomson Reuters and/or destruction of all copies of Thomson Reuters Data, including Personal Data, in Supplier's possession or control, including any information stored on backup media, in accordance with the terms of the DPA.

3. **Audit and Compliance requirement.** Thomson Reuters's audit and assessment rights, and Supplier's obligations related thereto, apply to an audit or assessment of Supplier's data security program and its controls. Without limiting the foregoing, Supplier shall also:

(i) Maintain current independent verification of the effectiveness of its technical and organizational security measures (ISO 27001, SOC 2, PCI DSS, HIPAA, and GDPR, PCI/DSS compliance if applicable, and annual Vulnerability Assessment and Penetration Testing report). The independent information security review must be performed at least annually.

(ii) Periodically review whether its systems and equipment storing or enabling access to Thomson Reuters Data, including Personal Data, comply with legal and regulatory requirements and contractual obligations.

(iii) Require any third parties processing Thomson Reuters Data to securely dispose of the information when no longer needed for the services they deliver.

(iv) Annually complete the cybersecurity risk assessment questionnaire, and any additional assessments following Security Incidents, using a third-party platform such as OneTrust. Supplier must also provide to Thomson Reuters all relevant documents related to information security controls, policies, procedures, SOPs, external audit reports, remediation plans, and evidence of control efficiency.

(v) Prohibit personally owned and managed equipment from being used to access or store Thomson Reuters Data.

4. **Incident Management.**

4.1 **IR Plan.** Supplier must implement and periodically test a formally documented incident management policy that includes:

(i) Clearly defined management and user roles and responsibilities.

(ii) Reporting mechanism for incidents and events affecting the security of Thomson Reuters Data (including Personal Data), including reporting of suspected unauthorised or unlawful access, disclosure, loss, alteration, and destruction of Thomson Reuters Data.

(iii) Procedures for assessment of, classification of, and response to, Security Incidents. Response procedures must be implemented within a reasonable timeframe and proportionate to the nature of the Security Incident and the harm, or potential harm, caused.

(iv) Procedures for notification to relevant authorities as required by Applicable Law and Thomson Reuters, within the timeframes specified by the law or in the Agreement.

(v) Procedures for forensic investigation and evidence preservation to fulfil Supplier's obligations under the Agreement.

(vi) A process for incident and resolution analysis designed to prevent the same, or similar, incidents from happening again.

(vii) Maintaining a security incident tracking system that documents and describes relevant information for each Security Incident affecting Thomson Reuters Data throughout its lifecycle, such as incident type, details, whether there was a data breach, the data affected, remediation actions taken, etc.

(viii) Timely informing Thomson Reuters of the measures taken or proposed to mitigate, contain, remediate, and fully investigate the Security Incident and provide a detailed report.

(ix) Supporting any investigation (e.g. by Thomson Reuters, law enforcement or regulatory authorities) that involves Thomson Reuters Data. Forensic procedures must be developed to support incident investigation.

(x) Assigning at least one dedicated point of contact with whom Thomson Reuters may communicate regarding the Security Incident 24 hours a day, 365 days a year.

(xi) Contractually bind all its Subprocessors who have access to Thomson Reuters Data and/or the Thomson Reuters network to adhere to the same incident management terms contained in this Section.

4.2 **Reporting Incidents to Thomson Reuters.** Supplier, without delay (and, in any event, within 48 hours) after becoming aware of or reasonably suspecting a Security Incident, shall provide notice to Thomson Reuters of such Security Incident, with additional notice to vendor_reportincident@thomsonreuters.com and the applicable Thomson Reuters

Procurement contact. Supply shall continue to update its notice until such time as the Security Incident is fully remediated.

4.3 **Immediate Response; Suspension.** In light of a potential or actual Security Incident involving Supplier, Thomson Reuters shall have the right to (but is not obligated to) suspend its use of Supplier's Solutions and/or suspend any access by Supplier or its personnel to Thomson Reuters systems or Thomson Reuters Data until Thomson Reuters receives adequate assurances, in Thomson Reuters's sole discretion, that the Security Incident has been fully contained and remediated by Supplier and that Supplier is otherwise in compliance with its privacy and security requirements under the Agreement (including the DPA and DSA). Supplier agrees that: (a) Thomson Reuters shall not be liable to Supplier or any other party for suspending such access or connections; (b) Supplier shall not charge Thomson Reuters for or, if Thomson Reuters already paid Supplier, shall refund to Thomson Reuters any fees or other amounts payable or paid to Supplier covering the time in which such access or connections were suspended; and (c) Thomson Reuters's right to suspend such use or access shall not relieve Supplier of its own obligations under the Agreement, including if the nature of the Security Incident warrants Supplier to proactively suspend its products or services or access to Thomson Reuters systems in order to contain or mitigate the Security Incident.

4.4 **Cooperation.** Upon request, Supplier shall: (a) reasonably cooperate to seek criminal prosecution or recovery in civil court (including for injunctive or other equitable relief) against any third party deemed responsible or complicit in the Security Incident; (b) reasonably cooperate to protect Thomson Reuters's or other third parties' (including Thomson Reuters's customers') rights relating to the use, disclosure, protection, and maintenance of the relevant Thomson Reuters Data; and (c) notify Data Subjects, Thomson Reuters customers, the public, and/or regulatory agencies or other third parties of such Security Incident (but only to the extent requested by Thomson Reuters and only using the form and content as finally approved by Thomson Reuters), and provide Data Subjects with credit monitoring or other protections requested by Thomson Reuters. Supplier shall bear all costs related to a Security Incident or to Supplier's breach of its obligations under this Agreement (including the DPA and DSA), including any costs to conduct an investigation, costs to notify consumers and others and to provide credit monitoring or other concessions to such persons or parties, and all fines, penalties, claims, suits, or any losses.

5. BUSINESS CONTINUITY AND DISASTER RECOVERY.

Supplier must have a management approved and maintained business resiliency program and must perform business continuity risk assessment activities to determine relevant risks, threats, impacts, likelihood and required controls and procedures which includes:

(i) Annual test and review of Business Continuity and Disaster Recovery (BC/DR) plans to validate the ability to restore availability and access to Thomson Reuters Data in a timely manner, in the event of a physical or technical incident that results in loss or corruption of Thomson Reuters Data.

(ii) Business Impact Assessment (BIA) to identify critical systems and corresponding recovery point objectives (RPO) and recovery time objectives (RTO).

(iii) Clearly defined roles and responsibilities.

(iv) Backup and restoration procedures that include sanitation, disposal or destruction of data stored at any alternate site.

(v) Overall management of critical response and recovery must include notification and escalation to customers/clients.

(vi) Backups containing customer data must be stored in an environment where the security controls protecting them are equivalent to production environment security control.

6. **AI/ML CONTROLS.** Without limiting Subsection 2.1.1 of the DPA and where Supplier's Solutions to Thomson Reuters include the use of AI/ML models (including Large Language Models (LLMs) or where Thomson Reuters Data is used in connection with AI/ML, the following additional security controls governing such models or such use of such data:

6.1 **Data Security:**

(i) *Encryption:* Supplier shall implement strong data encryption (at rest and in transit), in which (a) data at rest must be encrypted using a minimum of AES 256 or similar/latest standards regardless of hosting model, and (b) data in transit must be encrypted using Transport Layer Security (TLS) 1.2 version as a minimum, or as currently defined in the NIST Cryptographic Standards and Guidelines (e.g., NIST SP 800-52 Rev 2 guidelines for TLS implementations).

(ii) *Access Control and Authentication:* Supplier shall implement multi-factor authentication (MFA), applying principle of least privilege, role-based access control (RBAC) and audit and review access control on, at least, a quarterly basis.

(iii) *Compliance:* Supplier shall comply with all Applicable Laws, including, but not limited to, data privacy, security, and ethical standards governing LLMs, when developing, training, testing, and deploying LLMs, as well as when such LLMs Process Thomson Reuters Data.

(iv) *Zero Data Retention:* For clarity, the parties agree that the prohibitions set forth in Subsection 2.1.1 of the DPA: (a) apply to LLMs; and include that Supplier shall handle all API traffic from Thomson Reuters with confidentiality ensuring that no Thomson Reuters Data is logged or retained, including for abuse detection.

6.2 **Model Security:**

(i) *Encryption:* Supplier shall implement strong model encryption (at rest and in transit), in which (a) at rest encryption using a minimum of AES 256 or similar/latest standards regardless of hosting model, and (b) in transit encryption using Transport Layer Security (TLS) 1.2 version as a minimum, or as currently defined in the NIST Cryptographic Standards and Guidelines (e.g., NIST SP 800-52 Rev 2 guidelines for TLS implementations).

(ii) *Access Control and Authentication:* Supplier shall implement multi-factor authentication (MFA), applying principle of least privilege, role-based access control (RBAC) and audit and review access control on, at least, a quarterly basis.

(iii) *Versioning and Change Management:* Supplier shall maintain version control for all AI/ML models, implement change management processes for model updates, and keep detailed logs of all changes and updates to the model.

(iv) Input Validation and Sanitization: Supplier shall implement strong input validation, including monitoring of potentially harmful prompts or anomalous input patterns, to prevent prompt injection attacks; and sanitize inputs to prevent potential security vulnerabilities.

(v) *Business Continuity and Disaster Recovery:* Supplier shall develop and maintain plans for business continuity in case of AI/ML model failure or compromise, including implementing robust backup and recovery processes.

(vi) *Third-Party Risk Management:* Supplier shall conduct appropriate due diligence on any third-party AI/ML models it procures or any third-party services that utilize AI/ML.

(vii) Secure Development: Supplier shall develop, test, train, and deploy all AI/ML models using industry best secure model training and data management practices, including validation of protections against model interference, data poisoning, bias, and hallucinations.

(viii) Red Teaming: Supplier shall conduct regular, and no less than annual, 'Red Team' exercises on its AI/ML models; and Supplier shall remediate all findings and do so in accordance with the timelines outlined in Section 2.5 of this DSA.

7. **RESPONSIBILITY FOR PERSONNEL.** Supplier shall be responsible for its personnel's compliance with the terms of the Agreement and with its standard policies and procedures. Supplier personnel are responsible for appropriately handling all confidential data. Supplier shall provide information security training to all personnel and ensure Subprocessors receive such training on the privacy and security requirements of the Agreement upon hire and annually; and shall maintain a disciplinary process to address any violations of the Agreement (including any unauthorized access, use, alteration, loss, or disclosure of Thomson Reuters Data) by any Supplier personnel.

EXHIBIT B: DIGITAL ADVERTISING ADDENDUM

In addition to the other terms and conditions of the DPA (including the DSA), the following terms and conditions also apply to any Solutions provided by Supplier related to Digital Advertising:

1. **Tracking Technologies on TR Properties.** Supplier shall not utilize tracking technologies (including cookies, pixels, beacons, JavaScript) or any technology that collects online identifiers or Personal Data (collectively, "***Tracking Technologies***") on Thomson Reuters's digital properties (including websites and mobile applications) except as permitted by Thomson Reuters in writing.

2. **Tracking Technologies.** Supplier shall utilize Tracking Technologies, whether on a Thomson Reuters or third-party digital property, only in strict accordance with both (a) the relevant privacy statement or other notice that apply to such properties and (b) Applicable Law. Without limiting the foregoing, if Applicable Law requires individuals to provide prior opt-in consent before "dropping, "setting", "firing", or otherwise utilizing Tracking Technologies, then Supplier shall not utilize such technologies until that Data Subject has provided the required opt-in consent.

3. **Opt-Outs.** With respect to the use of Tracking Technologies or Personal Data, if a Data Subject either (a) does not consent or revokes their consent (or the consent string otherwise has a null/zero value) when consent is required by Applicable Law or is otherwise collected, or (b) opts-out of the Sale, the Sharing, or any other further Processing of their Personal Data, then Supplier shall only send a legally-compliant advertisement to that Data Subject as a Processor to Thomson Reuters and shall not Process that Data Subject's Personal Data (including, without limitation, serving personalized advertisements to that Data Subject or disclosing that Data Subject's information to third parties). Supplier shall flow down these requirements to all third parties who use Tracking Technologies, Process such Data Subject's Personal Data, or otherwise must abide by such choices in order for Supplier to fully effectuate those choices.

4. **Automated Choices.** Supplier shall abide by all preferences or other choices made by any Data Subjects concerning the use of Tracking Technologies or their Personal Data, including choices made to limit the use of Tracking Technologies or signal the Data Subject's opt-in/opt-out preferences via any technology (including, without limitation, the Global Privacy Control (GPC)), browser settings, or other opt-out preference signals.

5. **Digital Advertising Compliance Frameworks.** Supplier represents and warrants, on a continuing basis, that it participates in the Europe Transparency and Consent Framework ("***TCF***"), the Canada TCF, and the U.S. Multi-State Privacy Agreement ("***MSPA***") frameworks, as published by the IAB. Supplier shall adhere to the then-current requirements of each of the foregoing frameworks. To the extent Supplier publicly publishes the fact that it complies with any other data protection or advertising frameworks, Supplier represents and warrants, on a continuing basis, that it participates in and adheres to the requirements of such frameworks.

6. **Second- & Third-Party Data.** Supplier shall only Process each Data Subject's Personal Data collected directly by Supplier or collected from a third party solely to the extent permitted by Applicable Law. Without limiting the foregoing, Supplier shall only combine Thomson Reuters Data with Personal Data collected directly by Supplier or collected from a third party, where (a) expressly permitted by Thomson Reuters, (b) necessary to provide the Solutions, and (c) where all Personal Data was collected in accordance with Applicable Law and where such combination of data and further use of the combined data set does not violate Applicable Law.

7. **Transparency & Reporting**. Upon request, Supplier shall provide all reasonably requested information and reporting concerning its data processing activities related to Digital Advertising, including the use of Tracking Technologies and the handling of opt-in/opt-out preferences.

Previous Version (No Longer in Effect):

- *Supply Chain Data Protection Agreement v09-2021*[4]

[4] Link: https://www.thomsonreuters.com/content/dam/ewp-m/documents/thomsonreuters/en/pdf/global-sourcing-procurement/supply-chain-data-protection-agreement-v09-2021.pdf