THOMSON REUTERS DATA SECURITY ADDENDUM

This Data Security Addendum (the "**Addendum**") amends the Agreement between Thomson Reuters and Customer and sets out the obligations of both parties regarding the security of Customer Data in connection with the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum will take precedence only with respect to the security of Customer Data. Customer will mean the same as "Customer", "Client", or "you"; and Thomson Reuters will mean the same as "us", "we", "TR", or "Thomson Reuters", as the terms may be used in the Agreement.

1. INFORMATION SECURITY PROGRAM

1.1 Thomson Reuters will maintain an information security program that adopts the International Organization for Standardization (ISO/IEC 27002:2022) and/or the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The program will include, but is not limited to, the following components:

(i) Information security policy framework;

(ii) Program documentation;

(iii) Auditable controls;

(iv) Compliance records; and

(v) Appointed security officer and information security personnel.

1.2 Thomson Reuters will establish and maintain information security policies designed to protect the confidentiality and integrity of Customer Data hosted in the Services, which will include the following:

(i) Policies to restrict access to Customer Data only to authorized Thomson Reuters personnel and subcontractors;

(ii) Policies requiring the use of user IDs, passwords, and multi-factor authentication by Thomson Reuters personnel to access Customer Data;

(iii) Policies requiring connections to the internet to have commercially reasonable controls to help detect and terminate unauthorized activity prior to the firewall maintained by Thomson Reuters;

(iv) Policies requiring performance of periodic vulnerability assessments;

(v) Policies for the use of anti-malware and patch management controls to help protect against virus or malware infection and exploitation of security vulnerabilities; and

(vi) Policies and standards for the use of auditable controls that record and monitor activity.

1.3 Thomson Reuters will train and communicate to Thomson Reuters personnel its defined information security principles and information security policies and standards in accordance with the following:

(i) Applicable Thomson Reuters personnel will be required to take training, both at hire and on a regular basis, in information security practices and the correct use of information processing facilities to minimize possible security threats;

(ii) Applicable Thomson Reuters personnel will be instructed to report any observed or suspected threats, vulnerabilities, or incidents to our Security Operations Center; and

(iii) Thomson Reuters information security personnel will be made aware of reported information security threats and concerns and will support the Thomson Reuters information security policy in the course of their normal work.

1.4 Thomson Reuters will be responsible for its personnel's compliance with the terms of the Agreement and with Thomson Reuters standard policies and procedures. Thomson Reuters will maintain a disciplinary process to address any unauthorized access, use, or disclosure of Customer Data by any Thomson Reuters personnel.

1.5 Thomson Reuters will maintain a formal plan for incident response to promptly respond to suspected or confirmed breaches of Customer Data in accordance with regulatory and legal obligations.

1.6 Thomson Reuters policy with respect to user IDs and passwords for Thomson Reuters personnel accessing Thomson Reuters systems includes, but is not limited to, the following components:

(i) Each user has a unique account identifier or user ID;

(ii) Each user ID or account is assigned a password;

(iii) User IDs are added, modified, and deleted in accordance with Thomson Reuters-approved account management processes;

(iv) Verification of user identity before password resets;

(v) Passwords must conform to defined criteria that include length, complexity requirements and limitations on reuse;

(vi) User IDs, passwords, and tokens are not shared or used by anyone other than the user to whom it was assigned;

(vii) Temporary or default passwords are set to unique values and changed after first use;

(viii) User ID password changes are required at least every ninety (90) days;

(ix) Failed and repeated access attempts are locked for a reasonable and appropriate duration;

(x) Idle sessions are locked after a commercially reasonable period of time; and

(xi) User IDs are disabled after personnel termination.

2. DATA SECURITY CONTROLS

2.1 Application Strategy, Design, and Acquisition.

(i) Thomson Reuters will inventory applicable applications and network components and assess their business criticality.

(ii) Thomson Reuters will review critical applications regularly to ensure compliance with industry and commercially reasonable security standards.

2.2 Anti-Virus and Anti-Malware.

(i) Thomson Reuters will implement and configure industry standard anti-virus and anti-malware software on systems holding or processing Customer Data for regular signature updates.

(ii) Thomson Reuters will implement threat management capabilities designed to protect systems holding or processing Customer Data.

2.3 Network Security.

(i) Thomson Reuters will configure network devices (including routers and switches) according to approved lockdown standards.

(ii) Thomson Reuters will segregate the data center networks into separate logical domains with the network security controls approved by its security personnel.

2.4 Web and Application Security.

(i) Thomson Reuters will maintain commercially reasonable security measures for internet-accessible applications, including:

a. Implementing processes for developing secure applications;

b. Performing pre-deployment and ongoing security assessments of internet-accessible applications;

c. Developing internet-accessible applications based on secure coding guidelines such as those found in the Open Web Application Security Project (OWASP)

Development Guide; and

d. Validating the input, internal processing, and output of data in internet-accessible application(s).

(ii) Thomson Reuters will implement a change management process for documenting and executing operational changes in Services.

2.5 Compliance.

(i) Thomson Reuters will establish and adhere to policies that comply with laws and regulations that are applicable to Thomson Reuters and its provision of Services. Thomson Reuters does not determine whether Customer Data includes information subject to any specific law or regulation and compliance with any such law or regulation is the sole responsibility of the Customer.

(ii) To the extent legally permitted, Thomson Reuters will endeavor to notify Customer promptly after Thomson Reuters receives correspondence or a complaint from a government or regulatory official or agency related to the security of Customer Data. For purposes of the foregoing, a correspondence or complaint excludes normal customer service correspondence or inquiries.

2.6 Physical and Environmental Security.

Thomson Reuters Services will be housed in secure facilities protected by a secure perimeter, with generally accepted industry standard security barriers and entry controls for providers of similar services, including:

(i) Such Thomson Reuters facilities will be physically protected from unauthorized access, damage, and interference;

(ii) Access to such facilities will be logged and logs will be maintained;

(iii) Procedures will be maintained for visitors and guests accessing such Thomson Reuters facilities; and

(iv) Thomson Reuters will employ physical safeguards designed to protect Thomson Reuters Services systems from security threats and environmental hazards.

2.7 Security Testing and Patching.

(i) Thomson Reuters will perform security testing for common security coding errors and vulnerabilities against systems holding or processing Customer Data in line with generally accepted industry standards.

(ii) Thomson Reuters will regularly scan systems holding or processing Customer Data for security vulnerabilities.

(iii) Thomson Reuters will follow a commercially reasonable and industry standard security patching process.

2.8 Exchange, Transfer, and Storage of Information.

(i) Thomson Reuters will ensure that all account usernames and authentication credentials are stored and transmitted across networks and protected with a minimum of 128 AES encryption. Thomson Reuters will not store user credentials in clear text under any circumstances. Customer Data will be encrypted at a minimum of 256 AES when in transit and at rest. Thomson Reuters will also use encryption for Customer Data transmitted across the public Internet or wirelessly, and as otherwise required by applicable laws. Thomson Reuters will hold such encryption keys in the strictest of confidence and limit access to only named individuals with a need to have access.

(ii) Customer Data will not be stored or transported on a laptop or any other mobile device or storage media, including USB, DVDs, or CDs, unless encrypted using a commercially reasonable encryption methodology. All electronic data transfers of Customer Data by Thomson Reuters will be transmitted via SFTP or other commercially reasonable encrypted

form.

2.9 Penetration Testing, Monitoring, Vulnerabilities.

(i) Thomson Reuters or an appointed third party may periodically perform penetration testing on the Thomson Reuters systems supporting the Services. Upon written request, Thomson Reuters will make available to Customer a summary of the outcome of such relevant penetration testing or an executive summary of the penetration testing results.

(ii) Thomson Reuters will monitor the relevant Thomson Reuters information systems for security threats, misconfigured systems, and vulnerabilities on an ongoing basis.

(iii) Thomson Reuters will classify any vulnerability findings identified as emergency, critical, high, medium, or low in accordance with generally accepted industry standards for providers of similar services, and in accordance with Thomson Reuters risk assessment policies. Although the actual timeframe needed to effect such remediation will depend on the nature of the finding, Thomson Reuters will undertake commercially reasonable efforts to correct vulnerabilities according to the following timeframes:

Vulnerability Classification	Definition	Remediation Goal
Emergency	A vulnerability that has a high probability of being widely exploited in a manner disruptive to normal business operations	Begin deployment of patches and mitigations promptly, without undue delay, and complete remediation activities within seven (7) days
Critical	A vulnerability that has a high probability of being exploited that could result in broad exposure of confidential information or disruption of service, but the nature of the vulnerability does not reach the level of an "emergency" risk	Without undue delay and in any event within thirty (30) days
High Risk	A vulnerability that has a reasonably high probability of being exercised that could allow broad exposure or compromise of confidential information or disruption of service	Without undue delay and in any event within sixty (60) days
Medium Risk	A vulnerability that has a medium probability of being exercised	Without undue delay and in any event within ninety (90) days
Low Risk	A vulnerability that has a low probability of being exercised	Best efforts to address vulnerability in accordance with Thomson Reuters risk management policies; depending on the scope of the vulnerability, correction may be addressed in the next scheduled update

2.10 Personnel Access. Thomson Reuters will implement controls designed to manage its personnel's access to systems supporting the Services to be granted on a need-to-know basis consistent with assigned job responsibilities, which may include the use of role-based access controls to help ensure appropriate access rights, permissions, and segregation of duties.

2.11 Segregation of Data. Thomson Reuters agrees that Customer Data hosted within the Services in a production environment is maintained so as to preserve logical segregation of Customer Data from data of others.

2.12 Data Removal, Deletion and Destruction. If not otherwise set forth in the applicable Agreement, upon conclusion or termination of the Services at the written request of the Customer, Thomson Reuters will securely destroy and, upon request, confirm the destruction of all copies of Customer Data in any electronic or non-electronic form, except (i) for backup or archival copies kept in the normal course of business, including as part of a defined data retention program; or (ii) to the extent necessary to comply with applicable law and regulations.

2.13 Adjustment of Data Security Controls. Thomson Reuters will evaluate and may adjust its data security controls in light of: (i) the results of testing and monitoring; (ii) any material changes to Thomson Reuters operations or business arrangements; (iii) the results of risk assessments performed; or (iv) any other circumstances that Thomson Reuters knows or has reason to know may have a material impact on its data security controls.

3. SECURITY QUESTIONNAIRES AND ASSESSMENTS

3.1 No more than once per calendar year, Customer may request Thomson Reuters in writing to complete an information security questionnaire, or by way of a secure portal, be provided with a pre-populated security questionnaire in an industry-recognized format. Thomson Reuters agrees to respond to such questionnaire as soon as commercially reasonable. Customers who purchase multiple products under one or more agreements will coordinate requests into a single questionnaire per calendar year. You agree that the information contained in such responses is the proprietary and confidential information of Thomson Reuters.

3.2 To the extent Thomson Reuters performs and makes available to customers an independent third-party assessment or certification with respect to that service (e.g., ISO 27001, SOC 2), upon Customer's request, Customer may review an available executive summary of the results of such security assessments for the Services containing Customer Data. You agree that the information contained in such assessment, certification, or executive summary is the proprietary and confidential information of Thomson Reuters.

4. NOTIFICATION OF SECURITY BREACH

4.1 Thomson Reuters will, without undue delay but in any event within seventy-two (72) hours, notify Customer of a Security Breach. Thomson Reuters agrees that it will not inform any third party of any Security Breach naming you without first obtaining Customer's prior written consent, unless (i) required by applicable law or regulation; or (ii) such disclosure is in furtherance of a Thomson Reuters security breach investigation or the execution of its response plan.

4.2 In the event of any such Security Breach, Thomson Reuters will take commercially reasonable measures and actions to remedy or mitigate the effects of the Security Breach and will perform a root cause analysis to identify the cause of such Security Breach.

4.3 Upon Customer's reasonable request, Thomson Reuters may provide documentation related to such Security Breach, including, to the extent known, a summary of the cause of such Security Breach and steps taken to remedy the Security Breach and to prevent a recurrence. Thomson Reuters will reasonably cooperate with Customer in seeking injunctive or other equitable relief against any third party deemed responsible or complicit in the Security Breach.

4.4 If legally permitted, in the event of a Security Breach, Thomson Reuters agrees to reasonably cooperate with Customer in protecting its rights relating to the use, disclosure, protection, and maintenance of Customer Data.

5. BUSINESS CONTINUITY AND DISASTER RECOVERY

Thomson Reuters will, at all times while the Agreement is in effect, maintain a Business Continuity and Disaster Recovery Plan. Thomson Reuters will perform periodic testing of its Business Continuity and Disaster Recovery Plan to confirm its effectiveness. Upon Customer request, Thomson Reuters will provide a high-level report about the outcome of its latest Business Continuity and Disaster Recovery Plan test.

6. SERVICES RESILIENCE

6.1 Thomson Reuters will use commercially reasonable efforts to restore the Services by having offline backups of application data, infrastructure components and configuration settings.

6.2 Thomson Reuters will use commercially reasonable efforts to protect Services that host or process Customer Data against denial-of-service attacks by implementing denial-of-service mitigation solutions.

7. SHARED SECURITY OBLIGATIONS

You agree that you are responsible for all transactions that occur on your account and that it is your responsibility to ensure that you and your users use unique usernames and strong passwords for each account used to access the Services. You agree that you and your users must hold in confidence all usernames and passwords used for accessing the Services, and each user must immediately change their username/password combinations that have been acquired by or disclosed to an unauthorized third party. You also agree to enroll and require your personnel and other users to enroll in multi-factor authentication ("MFA") where made available to you, and you are responsible for all transactions and other activity that would have been prevented by the proper use of MFA. Additionally, you will notify Thomson Reuters if you become aware of any unauthorized third-party access to Thomson Reuters data or systems and will use reasonable efforts to remedy identified security threats and vulnerabilities to your systems.

8. BACKGROUND CHECKS

Employment background checks serve as an important part of the Thomson Reuters selection process. Verifying background information validates a candidate's overall employability or an employee's suitability for a particular assignment. Depending on the country and position at issue, to the extent customary and permitted by law, all Thomson Reuters background checks may include identification verification, prior employment verification, criminal background information, global terror/sanctions checks, and education verification. Thomson Reuters agrees to use qualified information security personnel to perform data security services.

9. DEFINITIONS

(i) "**AI Functionality**" means the functionality within the Services that is powered by or otherwise enabled through artificial intelligence (AI).

(ii) "**Agreement**" means the underlying agreement between Thomson Reuters and Customer for the provision of Services that references and incorporates this Addendum.

(iii) "**Business Continuity and Disaster Recovery Plan**" means a business continuity, contingency and disaster recovery activation plan to minimize disruption in, and reinstate the operation of the use of, the Services by you due to a disaster or similar event.

(iv) "**Customer Data**" means all data, content, Prompts, and other materials uploaded or submitted to, or generated through the use of, the Services by or on behalf of Customer, excluding any Usage Information, Thomson Reuters Content, authentication or security information, billing or customer relationship information, and marketing information.

(v) "**Installed Software**" means the object code version of software (including any updates or upgrades thereto) provided by Thomson Reuters and authorized to be installed on a Customer device, as specified in the applicable Ordering Document.

(vi) "**Interface**" means any application programming interface (API), model context protocol (MCP) server or endpoint, software development kit (SDK), connector, library, webhook, or other technical mechanism that enables programmatic access to, interaction with, or retrieval of data or functionality from the Services.

(vii) "**Ordering Document**" means an order form, online order, or statement of work issued by Thomson Reuters and entered into by Customer specifying the Services and/or Professional Services to be provided.

(viii) "**Output**" means any data, content, or other materials generated by the AI Functionality of the Services and returned to Customer or its users in response to a Customer Prompt.

(ix) "**Professional Services**" means the professional services, such as consulting, integration, implementation, or training services, as may be described in the applicable Ordering Document.

(x) "**Prompt**" means any prompt, instruction, request, or query submitted by Customer to the AI Functionality of the Services for the purpose of generating an Output.

(xi) "**Security Breach**" means a confirmed breach of security that results in the unauthorized destruction, loss, alteration, disclosure of, or access to Customer Data where such breach of security is likely to result in a significant risk of harm to you or your Data Subject(s) or where Thomson Reuters is required by applicable data protection law to notify you thereof.

(xii) "**Services**" means the Thomson Reuters software and software-based services provided under the Agreement (including Installed Software, cloud, or software-as-a-service solutions), which may include access to and use of any Thomson Reuters Content provided under the Agreement. Services exclude Professional Services.

(xiii) "**Thomson Reuters Content**" means any data, information, documents, publications, databases, datasets, articles, analyses, or other materials made available by Thomson Reuters as part of the Services or contained within an Output, whether delivered electronically, through online platforms, via an Interface, or otherwise. Thomson Reuters Content excludes (i) software or software-based functionality, including AI Functionality; (ii) Customer Data; and (iii) any publicly available third-party web content or materials surfaced, retrieved, or summarized by AI Functionality or other automated features of the Services.

(xiv) "**Usage Information**" means data regarding access to and use of the Services generated or collected by Thomson Reuters (e.g., logs, diagnostics, performance/availability, feature use, support chatbots, device/technical information, and related metadata), excluding Customer Data.