THOMSON REUTERS®

Thomson Reuters Data Security Addendum (December 2022)

This Data Security Addendum (the "***Addendum***") will apply to the Services set forth in the applicable order form, order confirmation, statement of work, invoice, e-commerce confirmation or similar agreement issued by such Thomson Reuters entity or entities (each, in any form, an "***Ordering Document***") and is fully incorporated therein. In the event of a conflict between the terms and conditions of this Addendum and the Ordering Document, the terms and conditions of this Addendum will take precedence. For clarity, this Addendum replaces and supersedes any Thomson Reuters security obligations that are set forth in the Ordering Document, regardless of whether the Ordering Document was executed prior to or after this Addendum. Customer will be 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 Ordering Document.

1. INFORMATION SECURITY PROGRAM

1.1 Thomson Reuters will 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 will include, but is not limited to, the following components:

(i) Information security policy framework
(ii) Program documentation
(iii) Auditable controls
(iv) Compliance records
(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 Your Data hosted in the Services, which will include the following:

(i) Policies to restrict access to Your Data only to authorized Thomson Reuters personnel and subcontractors.
(ii) Policies requiring the use of user ID's and passwords to access Your 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.
(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 a designated point of contact.
(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 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.

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

1.6 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 accessing 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. 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.

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)
(iii) 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 Your Data for regular signature updates.
(ii) Thomson Reuters will implement threat management capabilities designed to protect systems holding or processing Your 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.
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 Audit & Compliance.

Thomson Reuters will establish and adhere to policies that comply with applicable laws. However, Thomson Reuters is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to Thomson Reuters. Thomson Reuters does not determine whether Your 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.

2.6 Physical and Environmental Security.

Thomson Reuters Services will be housed in secure facilities protected by a secure perimeter, with industry standard security barriers and entry controls, 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.
(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 Your Data in line with accepted industry standards.
(ii) Thomson Reuters will regularly scan systems holding or processing Your Data for security vulnerabilities and resolve findings within commercially reasonable and industry standard timelines.
(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 encrypt Your Data when in transit externally and at rest including any data backups with commercially reasonable encryption algorithms.
(ii) Thomson Reuters will also use encryption for Your Data being transmitted across the public Internet or wirelessly, and as otherwise required by applicable laws. This obligation will extend to Your Data downloaded to any external devices such as a removable storage device.
(iii) Thomson Reuters will (i) hold such encryption keys in the strictest of confidence, and (ii) limit access to only named individuals with a need to have access.

2.9 Penetration Testing.

Thomson Reuters or an appointed third party may periodically perform penetration testing on the Thomson Reuters systems supporting the Services. Thomson Reuters will classify any vulnerability findings identified in any such penetration testing as critical, high, medium, or low in accordance with generally accepted industry standards for providers of similar services, and Thomson Reuters will provide remediation in a commercially reasonable period of time, all in accordance with Thomson Reuters risk assessment policies. Although the actual timeframe needed to affect such remediation will depend on the nature of the finding, Thomson Reuters will endeavor to remediate all findings in alignment with the Thomson Reuters vulnerability remediation policy.

2.10 Data Removal, Deletion and Destruction.

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

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.

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 summary of the results of such security assessment for the Services containing Your Data.

4. NOTIFICATION OF SECURITY BREACH

4.1 Thomson Reuters will, within seventy-two (72) hours, notify Customer of a Security Breach.

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 reoccurrence. Thomson Reuters will reasonably cooperate with Customer in seeking injunctive or other equitable relief against any such person deemed responsible or complicit in the Security Breach.

5. BUSINESS CONTINUITY

Thomson Reuters will, at all times while this Agreement is in effect, maintain a Business Continuity Plan. Thomson Reuters will perform periodic testing of its Business Continuity Plan to confirm its effectiveness. Upon Customer request, Thomson Reuters will provide a high-level summary about its Business Continuity Plan.

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 Your Data against denial-of-service attacks by implementing denial-of-service mitigation solutions.

7. PASSWORD REQUIREMENTS

Password selection and management controls for accessing Your Data will include the following where available:

(i) Verification of user identify before password resets,
(ii) Password-complexity requirements based on commercially reasonable information security standards,
(iii) Temporary or default passwords are set to unique values and changed after first use,
(iv) Failed and repeated access attempts are locked for a reasonable and appropriate duration,
(v) Idle sessions are locked after a commercially reasonable period of time.

8. BACKGROUND CHECKS

Employment background checks serve as an important part of 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 as is 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.

9. DEFINITIONS

"**Business Continuity 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.

"**Professional Services**" means the implementation, customization, training, consulting or other professional services we provide, as may be described in the applicable Ordering Document.

"**RTO**" means recovery time objective.

"**RPO**" means recovery point objective.

"**Security Breach**" means a confirmed breach of security that results in the unauthorized destruction, loss, alteration, disclosure

of, or access to Your 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.

"**Services**" means the cloud computing services, software-as-a-service, online research services, Professional Services, as well as any products, including installed software, supplied by Thomson Reuters that are detailed in the applicable Ordering Document.

"**Usage Information**" means (i) data and information related to your use of Thomson Reuters products, Services, information, Documentation which is aggregated and anonymized, including statistical compilations and performance information related to the provision and operation of our Property and (ii) any information, data, or other content derived from your access to or use of the Services, but does not include Your Data

"**Your Data**" means information, data, and other content, in any form or medium, that is submitted, posted, or otherwise transmitted by you or on your behalf through the Services. For clarity, Your Data does not include any information belonging to Thomson Reuters or its licensors, including without limitation: any content provided by Thomson Reuters as part of the Services, authentication and security information, billing and customer relationship information, marketing information, and Usage Information.