EXHIBIT A: THOMSON REUTERS DATA SECURITY ADDENDUM

1. INFORMATION SECURITY PROGRAM.

1.1. **Information Security Program.** Thomson Reuters will maintain an information security program designed to protect the confidentiality, integrity, and availability of Customer Personal Data. The program includes, but is not limited to, the following components:

- 1.1.1. Information security policy framework;
- 1.1.2. Program documentation;
- 1.1.3. Auditable controls;
- 1.1.4. Compliance records;
- 1.1.5. Appointed security officer and information security personnel.

1.2. **Policies, Standards, and Guidelines.** Thomson Reuters will establish and maintain information security policies, standards, and guidelines designed to protect the confidentiality, integrity, and availability of Customer Personal Data hosted in the Services, which includes the following:

- 1.2.1. Policies to restrict access to Customer Personal Data only to authorized Thomson Reuters personnel and subcontractors;
- 1.2.2. Policies requiring the use of unique user ID's and passwords;
- 1.2.3. Policies requiring secure connections to the internet to have commercially reasonable controls designed to detect and terminate unauthorized activity prior to the firewall maintained by Thomson Reuters;
- 1.2.4. Policies requiring performance of regular vulnerability assessments of Thomson Reuters LAN, WAN, and critical application and network components;
- 1.2.5. Policies for the use of anti-malware and patch management controls designed to protect against virus or malware infection and exploitation of security vulnerabilities;
- 1.2.6. Policies and standards for the use of auditable controls that record and monitor activity.

1.3. **Training.** Thomson Reuters will train and communicate to its personnel the defined information security principles and information security policies and standards, including that:

- 1.3.1. Thomson Reuters personnel will be trained in information security practices and the correct use of information processing facilities designed to minimize possible security threats;
- 1.3.2. Security awareness training attendance reports will be maintained in the Thomson Reuters personnel's file or other compliance tracking tool;
- 1.3.3. Thomson Reuters personnel will be required to report any observed or suspected threats, vulnerabilities, or incidents to the designated point of contact;
- 1.3.4. Thomson Reuters information security personnel will be made aware of reported information security threats and concerns, and will be equipped to support the Thomson Reuters information security policy in the course of their normal work.

1.4. **Access Controls.** Thomson Reuters will manage its personnel access to systems supporting the Services in a manner that is designed to be granted on a need-to-know basis consistent with assigned job responsibilities.

1.5. **Business Continuity.** Thomson Reuters will develop business continuity plans, in which these plans will be tested and approved by Thomson Reuters management on a periodic basis.

1.6. **Vendor Risk Assessment.** Thomson Reuters will maintain a program for vendor risk assessment.

2. **DATA SECURITY CONTROLS.** In the context of the Agreement, Thomson Reuters will use commercially reasonable efforts to:

2.1. **Application Strategy, Design, and Acquisition.**

2.1.1. Inventory applications and network components that support provision of hosted services and assess their business criticality;

2.1.2. Perform Thomson Reuters standard security compliance review for acquired or developed applications;

2.1.3. Review critical applications at least annually for compliance with industry and commercially reasonable security standards.

2.2. **Anti-Virus and Anti-Malware.**

2.2.1. Implement and configure anti-virus and anti-malware software for regular signature updates;

2.2.2. Implement threat management capabilities designed to protect systems holding or processing Customer Personal Data.

2.3. **Network Security.**

2.3.1. Configure network devices (including routers and switches) according to approved lockdown standards;

2.3.2. Govern and monitor changes to network security controls (including firewalls) using change management standards;

2.3.3. Segregate data center networks into separate logical domains with the network security controls approved by Thomson Reuters security personnel.