**DATA PRIVACY AND SECURITY REQUIREMENTS ("DPSR")**

This DPSR is made a part of the agreement ("Agreement") between Bloomberg and Supplier. In the event of a conflict or inconsistency between the terms and conditions of the Agreement (including the NDA) and this DPSR, the terms and conditions of this DPSR shall prevail except as otherwise specifically set forth in this DPSR. Capitalized terms used and not defined in this DPSR shall have the meanings given in the Agreement. References to the Agreement in this DPSR include this DPSR and the NDA.

For purposes of the Agreement, Personal Data may include names, addresses, e-mail addresses, dates of birth, phone numbers, government identifiers such as Social Security or driver's license number, financial information such as account numbers and credit card information, personal health information and commentary or an opinion about a person. Personal Data includes the contents of all logs and any other materials generated by Supplier to the extent such logs or materials contain Personal Data. Personal Data shall be deemed to be Bloomberg Confidential Information, and shall be subject to the terms of the NDA except as otherwise specifically set forth in this Agreement, even if such Personal Data is publicly available.

1. **Supplier General Obligations.**

1.1 Representative. Supplier shall appoint a representative to act as a point of contact for Bloomberg and to be responsible for fully, accurately, and promptly responding to any Bloomberg inquiry or questionnaire regarding data privacy or security.

1.2 Compliance with Law. Supplier represents and warrants that is in compliance, and shall remain in compliance, with all applicable data protection, privacy and data security laws, regulations, guidelines and industry standards in effect during the Term (including any applicable laws, regulations, guidelines and industry standards in the jurisdiction where Supplier performs the Services), including in all material respects ISO/IEC 27002, ("Data Protection and Privacy Laws"). To the extent Supplier processes credit card payment information and/or provides a payment application in connection with the Services, Supplier represents and warrants that it is in compliance, and shall remain in compliance, with the most recent PCI-DSS and PA-DSS standards. To the extent Supplier processes Personal Data of individuals within the European Union, European Economic Area and Switzerland ("EU") in connection with the Services, Data Protection and Privacy Laws shall be deemed to include "EU Data Protection Laws", defined as: (i) prior to 25 May 2018 the UK Data Protection Act 1998 and the Data Protection Directive (95/46/EC) and (ii) on and after 25 May 2018, EU Regulation 2016/679 ("GDPR"), and any equivalent, replacement or similar legislation implemented in the United Kingdom after that date, whether in light of the United Kingdom's withdrawal from the European Union or otherwise. Supplier shall also:

(i) assist Bloomberg to comply with all Data Protection and Privacy Laws applicable to Bloomberg's use of the Service (including with respect to notifications to and prior consultations with relevant supervisory authorities and data protection impact assessments);

(ii) maintain any certifications required for its compliance with Data Protection and Privacy Laws for the term of the Agreement, and notify Bloomberg promptly if any such certifications expire without being renewed or become invalid;

(iii) ensure that neither Supplier nor the provision of Services violates, or causes Bloomberg or its affiliates to violate, any Data Protection and Privacy Laws and immediately inform Bloomberg if, in its opinion, carrying out an instruction from Bloomberg would cause a breach of a Data Protection and Privacy Law.

1.3 Instructions to Supplier. Supplier shall:

(i) take appropriate administrative, technical, organizational, and physical measures to protect against unauthorized or unlawful processing of Bloomberg Confidential Information and against loss of, destruction of, damage to, corruption of, unauthorized alteration to, loss of integrity of, commingling of, or unauthorized access to Bloomberg Confidential Information, and shall revise such measures upon the request of Bloomberg to ensure they are appropriate for the stated purposes and as otherwise may be required under the Agreement;

(ii) maintain written records of all categories of processing activities carried out on behalf of Bloomberg, and make such records available to Bloomberg on reasonable notice;

(iii) not de-identify or anonymize Bloomberg Confidential Information, and not take steps to aggregate Bloomberg Confidential Information;

(iv) not rent or sell Bloomberg Confidential Information for any purpose, including marketing; and

(v) unless required to do otherwise by applicable law, in which case Supplier shall provide prior notice to Bloomberg unless prohibited from doing so by law:

a) only process Bloomberg Confidential Information in accordance with Bloomberg's written instructions;

b) only collect, use, and disclose Bloomberg Confidential Information for the purpose of providing the Services in accordance with the Agreement;

c) provide Bloomberg with the means to update or erase Personal Data, or promptly update or erase the Personal Data within 30 days of Bloomberg's request; and

d) not collect, record, store, or otherwise process any Personal Data in connection with performing the Services other than the Personal Data provided to it by Bloomberg or its affiliates.

1.4 Subprocessors. References to subprocessors in this DPSR include any third party engaged by Supplier, including affiliates and subcontractors, which has access to or processes Bloomberg Confidential Information in connection with the Services. Supplier shall:

(i) obtain Bloomberg's consent prior to engaging any subprocessor or making any change to an existing subprocessor;

(ii) ensure that its contract with any subprocessor includes: (a) terms at least as protective of Bloomberg Confidential Information as those in the Agreement; and (b) any terms required by Data Protection and Privacy Laws applicable to Bloomberg or Supplier;

(iii) indemnify Bloomberg against any costs or damages incurred in connection with subprocessor's processing of Bloomberg Confidential Information;

(iv) as between Bloomberg and Supplier, be responsible for all fees and costs related to each subprocessor meeting all of Bloomberg's requirements hereunder;

(v) remain liable for the performance of its obligations and responsibilities hereunder, including any warranties provided herein;

(vi) immediately notify Bloomberg of and assist Bloomberg with any investigation of an actual or potential violation of this Agreement by a subprocessor;

(vii) upon notice from Bloomberg, cease using a subprocessor to process Bloomberg Confidential Information and ensure that such subprocessor immediately returns

to Bloomberg or deletes all Bloomberg Confidential Information from all of subprocessor's systems.

1.5 Supplier Personnel. Supplier shall ensure its personnel ("Personnel") who have access to Bloomberg Confidential Information: (i) comply with the terms of this Agreement; (ii) are informed of the confidential nature of Bloomberg Confidential Information; (iii) are subject to and comply with appropriate contractual obligations of confidentiality with respect to any Bloomberg Confidential Information accessible to such Personnel; and (iv) receive industry best practice data protection, privacy and security awareness training before they are allowed to access Bloomberg Confidential Information and no less than annually thereafter. If Bloomberg notifies Supplier that Bloomberg Confidential Information is not to be processed by an individual person or group of people within Supplier's Personnel, Supplier shall immediately revoke such Personnel's access to Bloomberg Confidential Information, ensure that any copies of Bloomberg Confidential Information accessible to such Personnel are returned or securely destroyed, and instruct such Personnel to cease all processing of Bloomberg Confidential Information.

1.6 Bloomberg Resources. To the extent that Supplier's Personnel use Bloomberg's equipment, facilities, or services ("Bloomberg Resources") in connection with providing the Services, Supplier shall notify such Personnel that Bloomberg Resources shall be used solely for the purposes authorized by Bloomberg and that Bloomberg may monitor, access, and process their use of Bloomberg Resources: (i) to ensure that such use is limited to those purposes; or (ii) for any other purpose permitted by applicable law. Supplier acknowledges and agrees that Bloomberg may access such Personnel's use of Bloomberg Resources and disclose information about such Personnel's use of Bloomberg Resources with Supplier and other third parties.

1.7 Transfer. Supplier shall not transfer any Bloomberg Confidential Information to any jurisdiction outside the EU, if applicable, or the country in which Supplier will store Bloomberg Confidential Information without Bloomberg's prior consent. Without limiting the foregoing, Supplier represents, warrants and covenants that any cross-border transfer of Bloomberg Confidential Information complies with Data Protection and Privacy Laws, including on Bloomberg's request by confirming adherence to binding corporate rules, or with Bloomberg's prior consent, complying with another data transfer arrangement provided for under Data Protection and Privacy Laws (including EU Data Protection Laws, if applicable). If requested by Bloomberg, Supplier shall also obtain the necessary consents from and/or provide the necessary notifications to individuals required by Data Protection and Privacy Laws, to enable Bloomberg to process any Personal Data provided by Supplier in connection with the provision of Services, including to transfer such Personal Data to various jurisdictions around the world, including the United States. For the avoidance of doubt, "transfer" shall include the accessing of Personal Data from a jurisdiction other than where the Personal Data is stored.

1.8 Rights of Data Subjects. Supplier shall notify Bloomberg promptly and no later than five business days after receipt if Supplier receives a request from an individual for access to, or rectification or erasure of, Personal Data, or if it receives an objection from an individual to the processing of Personal Data. In the event Supplier or Bloomberg receives such a request or objection, Supplier shall promptly (and no later than five business days after receipt of the request from the individual or Bloomberg, as applicable): (i) provide Bloomberg with such information as Bloomberg may reasonably require to allow Bloomberg to respond to any such request or objection; and (ii) provide commercially reasonable assistance in relation to any such request or objection, including obtaining proper identification and verification from the individual. Supplier shall not disclose the individual's Personal Data or otherwise

respond directly to the individual without the prior consent of Bloomberg except as otherwise required by law. Supplier shall be responsible for all costs incurred in connection with an inability of Supplier to produce Personal Data, including any claim by the individual making the request or objection and any claim by a third party in connection with a disclosure under Section C.3 of the NDA (regarding legally compelled disclosure of Bloomberg Confidential Information).

1.9 Privacy Policies. Supplier agrees that any privacy policy it maintains that is relevant to the Services shall be consistent with its obligations under the Agreement, including the limitations placed on Supplier's collection, use, processing and disclosure of Bloomberg Confidential Information. Supplier shall provide any such privacy policy to Bloomberg prior to posting.

2. **Security Compliance and Administration.**

2.1 Information Security Program. Supplier represents and warrants that it shall maintain the confidentiality, integrity, availability and resilience of processing systems and services used to process Bloomberg Confidential Information and has implemented and shall maintain a comprehensive written information security program including administrative, technical, and physical safeguards appropriate to its business and the volume and sensitivity of Personal Data that it processes in connection with providing the Services, and that the program contains the following components:

(i) a designated individual or team of Personnel responsible for reviewing, maintaining, and updating the program (at least annually);
(ii) monitoring of the threat landscape for new internal and external risks to the controls designed to protect Bloomberg Confidential Information;
(iii) effective security policies and procedures governing Personnel's handling of Bloomberg Confidential Information;
(iv) an incident response plan in the event of a Security Incident, including mitigation, client communication, and post-incident review;
(v) a disaster recovery/business continuity plan that addresses ongoing access, maintenance and storage of Bloomberg Confidential Information, and security needs for back-up sites and alternate communication networks;
(vi) a data loss prevention program including controls to prevent loss of Bloomberg Confidential Information through personal email, portable storage devices (including portable hard drives, flash drives, and thumb drives), cloud storage platforms, and other means;
(vii) disciplinary measures for Personnel that fail to comply with the program; and
(viii) effective oversight of subprocessors, including regular security reviews.

2.2 Default Deny – Internet Accessibility. Supplier shall ensure that Bloomberg Confidential Information is not accessible from any Internet-facing applications or systems other than as strictly necessary to provide the Services.

2.3 Computer and Network Security. Supplier shall implement the following controls, at a minimum, with respect to the systems and networks used to process Bloomberg Confidential Information:

(ix) secure user authentication protocols, including: (a) effective control of user IDs and other identifiers; (b) a reasonably secure method of assigning and selecting strong passwords, or use of unique identifier technologies such as biometrics or token devices; (c) control of data security passwords to ensure that such passwords are kept in a location and format that does not compromise the

security of the data they protect; (d) restricting access to active users and active user accounts only; and (e) blocking access to user identification after multiple (10 or less) unsuccessful attempts to gain access through incorrect login credentials or any other control that may be placed on access for the particular system;

(x) secure access control measures that are based on the principles of segregation of duties and least privileged access that: (a) restrict access to Bloomberg Confidential Information to Personnel who need such information to perform their job duties; (b) provide access to Bloomberg Confidential Information that does not exceed what is required for Personnel to perform their function; (c) assign unique identifications and passwords, which are not vendor-supplied default passwords, to each individual person within Personnel, that are reasonably designed to maintain the integrity of the security of the access controls; (d) are regularly reviewed, audited, and updated to reflect system or Personnel changes;

(xi) replacement or disabling of vendor-supplied defaults for system passwords and other security parameters on any operating systems, software, or other systems;

(xii) encryption of all Bloomberg Confidential Information in transit over public or wireless networks, and at rest, including on Mobile Devices and backup media, using protocols approved by Bloomberg;

(xiii) regular and effective monitoring of systems and networks for evidence of unauthorized access or use and failure of security controls;

(xiv) up-to-date firewalls incorporating intrusion detection or prevention systems and effective network address / port filtering;

(xv) timely security patching, where the timeliness of the patching directly correlates to the severity of the vulnerability to be patched as described by the vendor issuing the patch and/or applicable industry guidance;

(xvi) up-to-date protection from malware and malicious code;

(xvii) disabling network-accessible features or functions not required to provide the Services; and

(xviii) regular and effective testing of the above controls to ensure their effectiveness.

2.4 Laptops and Mobile Computing Devices. Supplier shall not use laptops, tablets, smartphones, or any other mobile computing devices, ("Mobile Devices"), to process or store Bloomberg Confidential Information without Bloomberg's prior consent. If Bloomberg grants its consent, Supplier shall require Personnel to immediately report any loss or theft of any Mobile Device used to process or store Bloomberg Confidential Information, and shall ensure that such Mobile Devices are configured with the following minimum security controls, in addition to those specified directly above:

(xix) automatic locking of the Mobile Device following a period of inactivity of five minutes or less, where following such locking Personnel must unlock the Mobile Device using their unique login credentials;

(xx) whole-disk encryption using protocols approved by Bloomberg; and

(xxi) remote-wipe capability, which shall be exercised immediately following a reported loss or theft of any Mobile Device.

2.5 Portable Storage Devices. Supplier shall not use portable storage devices (including portable hard drives, flash drives, and thumb drives) to process or store Bloomberg Confidential Information without Bloomberg's prior consent. If Bloomberg grants its consent, Supplier shall require

Personnel to immediately report any loss or theft of such devices, and shall ensure that such devices are encrypted using protocols approved by Bloomberg.

2.6 Response to Known Vulnerabilities. In the event that Supplier becomes aware (including through its own reviews, third party reviews, and Bloomberg's reviews) of any vulnerabilities that permit unauthorized access to Bloomberg's Confidential Information, Supplier will immediately investigate, mitigate, and remediate such vulnerabilities. Supplier shall confirm to the best of its abilities whether there was unauthorized access to Bloomberg Confidential Information as a result of the vulnerability and, if there was such unauthorized access, shall notify Bloomberg in accordance with Section 5 of this DPSR.

2.7 Commingling of Data. Supplier shall not commingle Bloomberg Confidential Information with the data of any other customer of Supplier, and shall segregate Bloomberg Confidential Information through the use of physical or logical controls.

2.8 Physical Storage. If Bloomberg Confidential Information is stored on physical media (including paper documents and backup media), Supplier shall obscure or otherwise limit the use of the "Bloomberg" name on such media to the extent possible. Supplier shall control and protect access to any such media to avoid loss or damage, and shall ensure secure storage, transfer, exchange, and disposal of such media. Supplier shall ensure the facilities used to store any such media have: (i) electronically restricted ingress and egress points, and Supplier shall maintain logs of all access to and from the facilities; (ii) closed circuit camera recording equipment, and Supplier shall retain the video footage data of key document storage areas for at least 90 days; (iv) fire alarm and suppression systems; and (v) appropriate environmental controls (such as ventilation and humidity control).

2.9 Third-Party Data Centers. If Supplier uses a third party data center to host any application that processes, transmits or stores Bloomberg Confidential Information, Supplier shall ensure that all application and database servers are physically isolated within the data center and secured from unauthorized physical access. Physical and network access must be limited to Supplier's Personnel. Supplier shall ensure that Bloomberg Confidential Information remains segregated from other data stored in any shared environment and that use of any shared environment does not compromise the security, integrity, or confidentiality of Bloomberg Confidential Information.

2.10 Disruption of Bloomberg Systems. Supplier shall: (i) not knowingly take any actions that could disrupt or interfere with the operation of any Bloomberg system, and will take all steps necessary to prevent any such disruption or interference; and (ii) immediately notify Bloomberg of any critical vulnerability of any Bloomberg system discovered while performing the Services.

3. **Security Reviews by Bloomberg.**

3.1 Audit. Supplier shall promptly provide to Bloomberg upon request all information reasonably necessary to demonstrate its compliance with this DPSR. In addition, during normal hours of business and with reasonable prior notice to Supplier, Bloomberg or its designated third party may, at Bloomberg's expense, audit Supplier's processing and maintenance of Bloomberg Confidential Information and compliance with this DPSR and other terms of this Agreement: (i) once annually; (ii) any time a Security Incident has occurred; and (iii) if Bloomberg, in its sole discretion, reasonably believes that a Security Incident has occurred or Supplier is not in compliance with this Agreement. Such audit procedures shall occur through: (i) conversations with Supplier Personnel responsible for compliance with the applicable terms of this Agreement, who shall be made available by Supplier for such purpose; and (ii)

other customary audit procedures, including onsite visits to Supplier's offices, facilities, and data centers, network and application penetration tests, and a review of any security policies. Supplier shall, and shall ensure any subprocessors, assist and cooperate in the performance of such audit procedures.

3.2 Penetration Testing. Supplier shall engage an experienced third party to conduct regular penetration tests of its systems and networks that process and/or store Bloomberg Confidential Information. Such tests shall be conducted at least once annually, and following any major software release. Supplier shall make the results of such tests available to Bloomberg upon request.

3.3 Reports. Upon Bloomberg's request and at Supplier's expense, Supplier shall promptly provide to Bloomberg Supplier's most recent data security compliance reports on the systems, internal controls, and procedures relating to the Services (such as SSAE16 SOC1).

3.4 Regulators. Supplier shall promptly provide to Bloomberg upon request such information, cooperation and assistance as Bloomberg may require in order to determine Bloomberg's compliance with Data Protection and Privacy Laws, including with respect to data protection impact assessments and prior consultation with any relevant regulator regarding high risk processing. Should any regulatory body to which Bloomberg is subject require or request a security audit or review, Supplier shall cooperate with any such requirement or request with Bloomberg's full involvement (including Bloomberg's attendance at any related meetings with regulatory officials).

4. **Retention and Disposal.**

4.1 Definition of Secure Destruction. For the purposes of this DPSR, secure destruction refers to a process of rendering information permanently unreadable and unrecoverable through the use of best industry standard confidential information destruction techniques.

4.2 Retention During the Term. Bloomberg Confidential Information must be returned in the format and on the media requested by Bloomberg or securely destroyed within 90 days of the date that such Bloomberg Confidential Information is no longer reasonably required to perform the Services, unless otherwise required by law. Bloomberg Confidential Information shall not be retained by Supplier or any subprocessors beyond the expiration or termination of the Agreement, except as required by law or unless otherwise instructed by Bloomberg.

4.3 Instructions of Bloomberg. In addition to any other rights or remedies in the Agreement, Supplier and any subprocessors shall, unless otherwise required by law:

(xxii) immediately cease all processing of Bloomberg Confidential Information upon notice from Bloomberg;

(xxiii) update, delete, destroy, segregate, truncate, encrypt, mask, transfer, and/or provide to any third party designated by Bloomberg any Bloomberg Confidential Information stored or maintained by Supplier or any subprocessor, within 30 days of Bloomberg's request; and

(xxiv) securely destroy any Bloomberg Confidential Information specified by Bloomberg, including any associated backup copies, whether stored or maintained by Supplier or any subprocessor, within 10 days of Bloomberg's request.

4.4 Retention if Required by Law. If Supplier is required by law to retain Bloomberg Confidential Information, Supplier shall, to the fullest extent permitted by law: (i) notify Bloomberg of this requirement including the required retention period; (ii) store electronic copies of Bloomberg Confidential Information in encrypted offline storage (such as storage that is not network-connected or accessible) during such retention period; and (iii) store physical copies of Bloomberg Confidential Information in a securely locked container during such retention period. Unless Supplier has been given a date upon which Supplier will no longer be required by law to retain such Bloomberg Confidential Information, Supplier will periodically request such a date and inform Bloomberg as permitted by law. Upon the date that Supplier is no longer required by law to retain such Bloomberg Confidential Information, Supplier shall, to the fullest extent permitted by law, immediately resume compliance with its obligations under this Section and notify Bloomberg.

4.5 Certification. After the secure destruction of Bloomberg Confidential Information, Supplier and any subprocessors shall provide notify Bloomberg to acknowledge that all Bloomberg Confidential Information has been destroyed.

**5. Security Incident Response.**

5.1 Definition. "Security Incident" means any unauthorized or unlawful access to, use of, disclosure of, or any other compromise of Bloomberg Confidential Information or any material cause for reasonable concern about security as related to the Services. Within 24 hours of any confirmed or suspected Security Incident, Supplier shall notify Bloomberg of the Security Incident and any additional relevant details by email to breachnotice@bloomberg.com.

5.2 Incident Response. In addition to any rights or remedies in the Agreement, in connection with any confirmed or suspected Security Incident, Supplier shall immediately take all steps necessary or desirable to investigate, mitigate, and remediate the effects of the Security Incident and shall cooperate with Bloomberg in its investigation, comply with any directions of Bloomberg, and provide all material related to Bloomberg Confidential Information and the Services to satisfy Bloomberg's investigation and resolution process.

5.3 Supplier Actions Following Incident. Supplier shall:

(i) provide Bloomberg with assurance reasonably satisfactory to Bloomberg that the Security Incident will not recur;

(ii) not take any action that destroys or impairs any evidence with respect to the Security Incident;

(iii) appropriately document the Security Incident and the response; and

(iv) assist and cooperate with:

(a) any independent forensic investigation;

(b) any required or appropriate disclosure to affected entities, individuals, or regulatory bodies;

(c) any other remedial measures reasonably requested or required under any applicable law or regulation; and

(d) any response to regulatory inquiries, litigation, or other similar actions.

5.4 Confidentiality. All information exchanged in connection with a Security Incident shall be deemed to be the Confidential Information of the disclosing party. Supplier shall not disclose any impact on Bloomberg of any Security Incident without the prior consent of Bloomberg, unless otherwise

obligated by applicable law, in which case Supplier will provide Bloomberg with prior notice of its obligation. Notwithstanding anything to the contrary in this Agreement, Supplier understands and agrees that Bloomberg has the right to disclose Supplier's Confidential Information to third parties in order to investigate and resolve a Security Incident, provided that Bloomberg requires such third parties to treat the information confidentially. In addition to any rights or remedies in the Agreement, Bloomberg may immediately terminate the Agreement and/or any Service upon notice to Supplier, without any further liability or obligation to Bloomberg, if Bloomberg reasonably believes a Security Incident has occurred or is imminent.

5.5 Costs and Notification. Supplier shall be responsible for all costs related to or arising from any Security Incident, including investigating the Security Incident, tracking and recovering Confidential Information, and providing notifications (which may include remedies provided to individuals affected by the Security Incident that are legally required or consistent with standard industry practice) to: (i) all individuals affected by the Security Incident; and (ii) state, federal, or international law enforcement or regulatory bodies. The provision of such notifications, if any, including the content thereof, shall be solely at the discretion of Bloomberg.

**6. Survival.**

This DPSR and all provisions herein shall survive the expiration or termination of this Agreement and shall continue for so long as the Supplier processes or retains any Bloomberg Confidential Information.