

PRIVACY EXHIBIT TO
 PURCHASE ORDER TERMS AND CONDITIONS (“PO”)

1. **Scope of Applicability.** The Privacy Exhibit (“Exhibit”) is applicable for Products or Services where a Seller is processing Refinitiv Data provided by or on behalf of Refinitiv. The PO governs this Exhibit; where this Exhibit conflicts with the PO, the Exhibit governs.
2. **Definitions.** “BCR” means the binding corporate rules to which the Seller and its Affiliates may be party to, and which are both internally and externally binding for the benefit of data subjects, and have been approved by all relevant regulators. “Data Protection Laws” mean all applicable laws, standards and regulations governing the processing of Personal Information, as may be amended or enacted from time to time. “Personal Information” means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly. “Process (and its derivatives)” means any operation or set of operations that is performed upon Refinitiv Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. “Sensitive Personal Information” means any Personal Information that requires additional protection under applicable Data Protection Laws as a result of its sensitive nature, including, without limitation, information concerning an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, physical or mental health, sex life or orientation, criminal records, financial account numbers, account passwords or voice mail access codes, medical records, biometric and genetic information, date of birth 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). “Refinitiv Data” means all electronic data or information submitted or made available by Refinitiv, its agents, customers, suppliers, contractors, and outsourcers to Seller; Refinitiv Data includes Personal Information and Sensitive Personal Information.
3. **Data Security.** Unless otherwise agreed by Refinitiv and Seller, all Refinitiv Data is and shall remain the exclusive property of Refinitiv. Seller shall collect, use, access, maintain, and disclose or share Refinitiv Data only for the benefit of Refinitiv, and only to the extent strictly necessary to perform its obligations under this Exhibit and PO, or as otherwise required by law and only in accordance with documented instructions contained in this Exhibit or received from Refinitiv from time to time in writing. Seller may not otherwise use or modify the Refinitiv Data, merge it with other data, commercially exploit it, disclose it, transfer it across international borders or do any other thing that may in any manner adversely affect the integrity, security or confidentiality of such Refinitiv Data, other than as expressly specified herein or as directed by Refinitiv in writing. Furthermore, Seller shall not maintain a copy of any Refinitiv Data, and shall not otherwise remove or duplicate any Refinitiv Data hereunder except as allowed under this Exhibit, the PO, or by the express written permission of Refinitiv. Upon the PO termination, Seller shall return any Refinitiv Data under Seller’s care to the control of Refinitiv or, if authorized and by providing a written certification of such, shall discard, destroy, and otherwise dispose of Refinitiv Data, making such data unrecoverable, in a secure manner to prevent unauthorized handling of the Refinitiv Data consistent with Refinitiv policies, applicable industry standards and/or applicable law. Seller may retain a copy of Refinitiv Data only to the extent it is obliged to so by Data Protection Laws. In addition, in so far as Seller Processes any Refinitiv Data on behalf of Refinitiv, Seller shall implement and maintain current and appropriate technical and organizational measures to protect the Refinitiv Data against accidental, unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration, disclosure or access. Seller shall (i) oblige its employees, agents or other persons to whom it provides access to Refinitiv Data to keep it confidential in accordance with the PO; (ii) before transferring the Refinitiv Data to any sub-processors, require such sub-processors to enter into a written contract with Seller which imposes obligations equivalent to Seller’s PO obligations with respect to the Refinitiv Data (including as set out in this Exhibit). Seller shall ensure the sub-processor complies with such obligations (including by auditing or otherwise taking steps in accordance with good industry practice to confirm such compliance at least annually). Upon request from Refinitiv, Seller shall confirm the timing, scope and findings of any such audit or confirmation exercise. Seller consents to Refinitiv disclosing the existence and nature of this relationship as required by Data Protection Laws.
4. **Seller Data Privacy.** Seller shall: (i) not process Personal Information for purposes other than the PO purposes unless required by Data Protection Laws (or in the case of Personal Information originating solely from outside of the European Union, unless required by the laws of the country from which the relevant Personal Information originated). Where any such requirement is placed on Seller, it shall provide prior notice to Refinitiv unless the relevant law prohibits the giving of notice on important grounds of public interest; (ii) not allow Personal Information to be taken from Seller premises, copied, or downloaded unless approved by Refinitiv in writing and only when required to meet Seller’s obligations set forth in the PO; (iii) assist Refinitiv to comply with its own data security obligations under Data Protection Laws; (iv) use pseudonymisation and encryption of Refinitiv Personal Information, where appropriate; (v) inform Refinitiv if, in its opinion, Refinitiv instructions would be in breach of Data Protection Laws; (vi) provide reasonable assistance to Refinitiv to allow it to conduct privacy impact assessments and to respond to requests from individuals exercising their rights under Data Protection Laws; and (vii) on request from Refinitiv, provide evidence of its and its subcontractors’ compliance with the provisions of this Exhibit.
5. **European Union Personal Information.** Where Personal Information is located within, or originates from, the European Union (EU) or European Economic Area (EEA), Seller may transfer any such Personal Information to any country or territory outside the EEA. The parties hereby agree to the terms of 2010/87/EU Standard Contractual Clauses (SCC) approved by the European Commission. The Parties agree Refinitiv is the exporting organization and Seller is the importing organization. Clause 9 and 11 of the SCC shall be governed by the law of the Member State in which the data exporter is established. Relevant information for Appendix 1 of SCC (describing the data subjects, categories of data, and processing operations) and Appendix 2 of SCC (describing the technical and organizational security measures implemented by importer) are contained in the PO. Alternatively, transfers may be facilitated subject to Seller’s approved and maintained BCR, or where transfers involve an adequate country recognized by the EU authorities.
6. **Non-EU or Non-EEA Personal Information.** Where Personal Information is located in a non-EU or non-EEA country or territory that has enacted Data Protection Law(s) restricting transfers of or access to Personal Information, Seller shall cooperate with Refinitiv to execute any agreements and to implement all processes and measures that Refinitiv deems appropriate to comply with such country’s Data Protection Law(s).
7. **Opt-In Consent.** Where applicable to the services provided, Seller shall ensure that, in accordance with applicable law and/or Refinitiv policies and procedures, all Personal Information Processed on behalf of Refinitiv by Seller shall originate from individuals and entities (including, without limitation, contractors) who Seller has properly notified and who have provided appropriate consent to the collection, access, use, maintenance and/or disclosure of the Personal Information. Unless otherwise agreed in writing by Refinitiv and Seller, the appropriate type of consent shall be express (“opt-in”) consent.
8. **General Compliance.** The parties shall comply with all laws and regulations applicable to the services provided by the seller to Refinitiv under this Agreement (“Data Protection Laws”).
9. **Audit Rights.** Seller shall, at Refinitiv’ request, permit Refinitiv or its external advisers, and regulators of Refinitiv or its customers, (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit Seller’s data processing activities and those of Seller’s agents, affiliates and sub-processors, to verify that Seller is in compliance with its obligations under this Exhibit. The following provisions additionally apply to such audits: (a) Except in the case of urgency (including in the event of a request from a regulator, or an actual or suspected security breach, data loss or misappropriation of Refinitiv Data) and unless it would seriously hamper the purpose of the audit, Refinitiv shall use reasonable endeavors to give Seller at least five business days’ notice of when the audit will be conducted and an estimate of the audit’s duration; (b) Seller shall provide all reasonable assistance to, and co-operate with, the auditor. Seller shall provide access to premises, personnel and relevant systems, and copies of any relevant information; (c) Each party shall bear their own costs of audit, except where the auditor finds that Seller has materially breached this Exhibit, in which case Seller shall bear all costs of the audit; and (d) If the audit reveals material non-compliance with this Exhibit, Refinitiv may exercise its termination rights underneath the PO.
10. **Breach Notification.** Seller shall promptly notify Refinitiv in the event that it becomes aware of, or reasonably suspects, (i) any breach of Data Protection Laws by Seller or any of its sub-processors in connection with the PO; (ii) any breach of this Exhibit; or (iii) any unusual activity that represents an actual or potential security threat or security breach on devices or systems hosting Refinitiv Data or otherwise being used to deliver services. If any of the foregoing events occur, Seller shall conduct a thorough investigation of such incident, document the steps for any needed remediation, provide the results of its analysis to Refinitiv promptly following the investigation, and implement the needed remediation on the timescales specified by Refinitiv. Seller shall assign one or more Seller personnel, and communicate to Refinitiv the name(s) of such Seller personnel, to manage security breach communications. In the event of a breach, such Seller personnel will be available to Refinitiv 24 hours a day, 365 days a year, to facilitate and respond to issues related to any breach. Seller shall bear all costs that Refinitiv incurs related to a security breach or data protection incident arising from or related to Seller’s breach of its obligations under the PO and this Exhibit, including without limitation: costs to conduct an investigation, cost to notify consumers and others required by law or Refinitiv policy, and all fines and penalties.