

FACTSET VENDOR DATA PROCESSING AGREEMENT

By providing services to FactSet and/or any of its Affiliates (“FactSet”) that involve Processing of Personal Data (“Services”), Vendor agrees to this Vendor Data Processing Agreement (“VDPA”). If Vendor has a master agreement, purchase order, order form, statement of work, or other written agreement under which Vendor provides Services to FactSet (“Agreement”), this VDPA is incorporated by reference and, along with related Annexes attached and signed as part of the Agreement and deemed as Annexes to this VDPA, governs Vendor’s Processing of Personal Data for FactSet.

1. PURPOSE

In connection with the Agreement, FactSet may provide Personal Data to Vendor. The parties agree to comply with the following provisions with respect to any Personal Data transferred to or processed or accessed by Vendor pursuant to or in connection with the Agreement.

This VDPA applies automatically and without further action when Vendor Processes Personal Data for Customer. This VDPA supersedes any prior agreements entered into between FactSet and Vendor for the purpose of providing adequate safeguards for the protection of privacy and security of personal data. In the event of any conflict between the terms and conditions of this VDPA and the Agreement in connection with or related to the processing of personal data, the terms, and conditions of this VDPA shall govern and control. Except as modified below, the terms of the Agreement shall remain in full force and effect.

2. DEFINITIONS

- 2.1 **“Affiliate”** means an entity that owns or controls, is owned or controlled by or is under common control or ownership with either FactSet or Vendor (as the context allows), where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.
- 2.2 **“Authorized Sub-Processor”** refers to a Sub-Processor which is authorized by FactSet and which is defined and listed in Annex III of the Agreement.
- 2.3 **“Controller”** means an entity that determines the purposes and means of the processing of personal data.
- 2.4 **“Data Privacy Framework” or “DPF”** means the self-certifying program wherein a U.S. participating organization commits to the DPF principles thereby allowing the transfer of personal data from the EU, UK, or Switzerland to the U.S. This includes the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework and the Swiss-U.S. Data Privacy Framework.
- 2.5 **“Data Protection Laws”** means applicable legislation that applies to the processing of personal data, including but limited to : (i) the California Consumer Privacy Act of 2018 and any subsequent amendments (“CCPA”), (ii) all other applicable United States privacy laws and regulations, (iii) GDPR; (iv) UK GDPR; (v) Section 5(a) of the Federal Trade Commission Act (15 U.S.C § 45), and (vi) all applicable country-specific laws, regulations or directives that require a data processing/sharing agreement.

- 2.6** “**Data Subject**” means the identified or identifiable natural person to whom personal data relates.
- 2.7** “**FactSet Personal Data**” means all Personal Data obtained by, processed by or made available to Supplier in connection with or in relation to the Agreement, this VDPA, and/or the provision of any products or services to or on behalf of FactSet, including, without limitation, any Personal Data that relates to or could be associated with FactSet, its employees, customers, and/or other end users of FactSet’s products, services, websites, advertisements, or content. As between Vendor and FactSet, all FactSet Personal Data is and will be deemed to be and will remain the exclusive property of FactSet.
- 2.8** “**General Data Protection Regulation**” or “**GDPR**” means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
- 2.9** “**Personal Data**” means any data or information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, including information relating to an identified or identifiable natural person where such data or information is accessed in connection with the Services under the Agreement or otherwise Processed by Vendor or any Sub-Processor on behalf of FactSet.
- 2.10** “**Processing**” (and all verb tenses) means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- 2.11** “**Processor**” means the entity which Processes Personal Data on behalf of the Controller.
- 2.12** “**Restricted Transfer**” means where the EU GDPR or the UK GDPR applies, a transfer of Personal Data to a country outside of the European Economic Area or the UK, which is not subject to an adequacy determination by the European Commission.
- 2.13** “**Security Incident**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unavailability, disclosure of, use of, publication of, or access to, Personal Data transmitted or otherwise subject to this VDPA or the Agreement.
- 2.14** “**Standard Contractual Clauses (SCCs)**” are the most recent SCCs published by the EU Commission forming part of this VDPA when applicable for a restricted transfer to a third country.
- 2.15** “**Sub-Processor**” means a Processor or subcontractor engaged by Vendor or any other Processor.
- 2.16** “**Supervisory Authority**” means an independent public authority which is established by an EU member state pursuant to the GDPR.
- 2.17** “**UK GDPR**” means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act of 2018.

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

3. ROLES OF THE PARTIES

- 3.1 Controller and Processor.** The parties acknowledge and agree that with regard to the Processing of Personal Data, and as more fully described in Annex I of the Agreement, each FactSet Affiliate will serve as a Controller, and Vendor is the Processor and Service Provider with respect to Personal Data that Vendor Processes pursuant to or in connection with the Agreement.
- 3.2 Vendor Representation and Warranty.** Vendor represents and warrants that it has the authorization necessary to enter into this VDPA, and no consent, approval, or other action is necessary in connection with the execution or performance of this VDPA. Vendor further represents and warrants that it will perform all of its duties and obligations under this VDPA and will comply with all applicable Data Protection Laws in its protection of the security and privacy of FactSet Personal Data in the fulfillment of its obligations and otherwise in its rendering of Services pursuant to or in connection with the Agreement.
- 3.3 Compliance.** Vendor represents and warrants that it has created and maintains written guidelines to ensure its compliance with its obligations under this VDPA, will provide those written guidelines to FactSet upon request, and trains its personnel in relation to these written guidelines. Vendor will immediately notify the designated representative of FactSet if Vendor reasonably determines it cannot comply with its Data Protection obligations under applicable Data Protection Laws. Notwithstanding any other provision in this Agreement, FactSet have the right to terminate this Agreement with immediate effect by providing written notice to Vendor if Vendor notifies FactSet, or FactSet has reasonable grounds to believe, that Vendor is unable or unwilling to comply on an ongoing and permanent basis with any applicable Data Protection Laws or obligations.

4. PERSONAL DATA PROCESSING OBLIGATIONS

- 4.1 Data Protection Laws.** The rights and obligations of FactSet and FactSet Affiliates are set out in this VDPA, including the applicable Schedules and Annexes, and as expressly set forth in the Agreement. The subject matter of the Processing pursuant to this VDPA, its nature and purpose, and the type of Personal Data and categories of Data Subjects, and notice details are set forth in Annex I of the Agreement. The duration of the Processing shall correspond to the term of the Agreement, subject to the provisions of Section 9 below.
- i. Vendor Processing of Personal Data. Vendor shall treat Personal Data confidentially and shall Process Personal Data on behalf of and only in accordance with FactSet's documented instructions to the extent necessary for Vendor to provide the Services to FactSet pursuant to the Agreement.
 - ii. Use of Data. Vendor shall comply with Data Protection Laws as it relates to the Processing of Personal Data. Vendor shall not combine Personal Data with any other information, including Vendor's own information, either received on behalf of another person or entity or collected from its own interactions with a Data Subject, for any other purpose. Vendor may not retain, use, sell, rent, release, share, disclose, disseminate, make available, transfer, or otherwise

exchange or communicate by any means Personal Data (or any portion thereof) for monetary or other consideration other than the business purpose specified in the VDPA, Agreement or as otherwise permitted by law. Vendor shall require that any Sub-processor enter into a written agreement that binds them to the same or similar requirements in this section. For avoidance of doubt, Vendor is prohibited from retaining, using, or disclosing Personal Data outside of the direct business relationship with FactSet and from Sharing personal data as defined herein.

- iii. Assistance. Taking into account the nature of Processing and the information available to Vendor, Vendor will promptly comply with any request from FactSet or FactSet Affiliates to provide reasonable assistance and cooperation to FactSet in respect of its relevant obligations under the Data Protection Laws, including but not limited to Articles 32 to 36 of the GDPR at no charge to FactSet.
- iv. Vendor Personnel.
 - a. Confidentiality Obligations. Vendor ensures that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and have executed written confidentiality agreements no less protective than the terms of this VDPA as it relates to Personal Data.
 - b. Limited Access. Vendor warrants that access, and any other Processing of Personal Data is limited exclusively to those personnel of Vendor authorized hereunder for Processing to perform Services to FactSet in accordance with the Agreement.
- v. Subcontractors or Sub-Processors. Vendor and Vendor's Subcontractors or Sub-Processors shall: (i) keep confidential all such FactSet Personal Data which it accesses or otherwise Processes pursuant to the terms of the Agreement; and (ii) limit access to such FactSet Personal Data only to those of its employees who have a need to access such FactSet Personal Data to perform their job functions, and to ensure that those employees are trained with respect to the obligations imposed by this VDPA and sign an undertaking to comply with these obligations as described herein.
- vi. Security.
 - a. Measures. Vendor warrants that it has implemented and shall maintain appropriate technical and organizational measures to protect Personal Data against accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure, and access or any other Personal Data Breach ("Security Measures"), as described in the FactSet Security Addendum, as applicable and if so attached to the Agreement, including but not limited to:
 - (i) the pseudonymization and encryption of Personal Data;
 - (ii) assurance of the ongoing confidentiality, integrity, availability, and resilience of all Processing systems that Process Personal Data;
 - (iii) to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
 - (iv) the regular testing, assessment, and evaluation of the effectiveness of the Security Measures.

vii. Agents and Sub-Processors.

- a. General Authorization. FactSet agrees that Vendor may use Authorized Sub-Processors (as initially listed in Annex III of the Agreement) to Process Personal Data to the extent necessary for Vendor to fulfill its contractual obligations under this VDPA or to provide certain services on Vendor's behalf.
- b. Sub-Processor Obligations. Vendor will not disclose or transfer Personal Data to any third-party, without the prior permission of FactSet given in writing or via email or other electronic means, except to the extent that a disclosure or transfer is required by law.
- c. Objection Right. FactSet may object to the use of a new Sub-Processor on a reasonable and legitimate basis. In the event FactSet objects to a new Sub-Processor, FactSet shall provide written notice to Vendor via the contact information provided in this VDPA outlining FactSet's specific concerns about the new Sub-Processor in order to give Vendor the opportunity to address such concerns. Vendor may, at its sole discretion: (i) not appoint the Sub-Processor and/or propose an alternate Sub-Processor; (ii) take the steps to address FactSet's specific concerns and obtain FactSet's written consent to use the Sub-Processor; or (iii) make available to FactSet the Vendor Product(s) without the particular aspect that would involve use of the objected to Sub-processor, and refund FactSet any pre-paid fees for such Services and/or Products on a pro-rata basis. If Vendor is unable or determines in its reasonable judgement, that it is commercially unreasonable to do any of the options in Section 4.1.vii.c(i)-(iii), FactSet may terminate the Agreement.
- d. Liability. Vendor will remain fully liable and responsible for the acts or omissions of all Sub-Processors to the same extent Vendor would be responsible for its own acts or omissions.

5. SECURITY INCIDENTS

- 5.1 **Notification of Personal Data Breach.** Vendor shall immediately notify FactSet, and in no case later than twenty-four (24) hours of becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Vendor or its Sub-Processors ("**Personal Data Breach**"). Notification of Personal Data Breaches will be delivered in writing to the contact information provided in Agreement.
- 5.2 **Investigation of Data Breach.** Vendor will investigate and remediate the Personal Data Breach or Security Incident and will provide FactSet, as soon as reasonably possible, with assurances satisfactory to FactSet that the Personal Data Breach or Security Incident has been remediated and will not reoccur.
- 5.3 **Full Cooperation.** Vendor will fully cooperate with FactSet in the handling of any Personal Data Breach or Security Incident, including without limitation any investigation, reporting, or other obligations required by Data Protection Laws, or as otherwise required by FactSet and will work with FactSet to otherwise respond to and mitigate any damages caused by the Personal Data

Breach or Security Incident. Vendor shall reimburse FactSet for all costs incurred in responding to and/or mitigating damages caused by a Personal Data Breach or Security Incident.

- 5.4 Communication.** Vendor is prohibited from communicating with any individual or third-party (other than law enforcement and except as required by applicable law) regarding any Personal Data Breach or Security Incident in any manner that identifies FactSet without the express prior written consent of FactSet.

6. PERSONAL DATA TRANSFER OBLIGATIONS

- 6.1 Instructions.** For the purposes of this VDPA, the parties agree that the following is deemed an instruction given by FactSet to Vendor to Process Personal Data: (a) Processing in accordance with the Agreement; (b) Processing to comply with other reasonable instructions provided by FactSet (e.g., via email) where such instructions are consistent with the terms of the Agreement; and/or (c) Processing in accordance with instructions from FactSet.

6.2 Transfers of Personal Data to Third Countries.

- i. Regions. FactSet may specify the location where FactSet Personal Data will be Processed in the Agreement ("Region"). Except as necessary to provide the Services in the Regions requested by FactSet, or as necessary to comply with Applicable Law, Vendor will not transfer Personal Data from FactSet's selected Region. Vendor warrants that a transfer of Personal Data to a third country shall take place only in compliance with Data Protection Laws. Where required, Vendor shall ensure that a lawful data transfer mechanism is in place prior to transferring Personal Data from one country to another. Lawful data transfer mechanisms include but are not limited to the execution and implementation of Standard Contractual Clauses or a proven participation of Vendor in the Data Privacy Framework for US based vendors. Without limiting the foregoing, Vendor shall take all appropriate additional measures necessary to ensure an adequate level of data protection for any Personal Data transferred from one country to another.

6.3 Audits and Certifications.

- i. Data Protection Audits. At least annually, Vendor will allow for and contribute to reasonable audits and inspections by FactSet, either by FactSet itself, its designated auditor, or an independent auditor designated by Vendor and agreed upon by FactSet. The audit will confirm Vendor's compliance with applicable Data Protection Laws and Vendor will provide a report of the audit to FactSet at its request.
- ii. Security Audits. In addition to the rights set forth in the Agreement hereto, the parties agree that audits and certifications will be satisfied by the following, subject at all times to any requirements of the applicable Supervisory Authority.
- a. Summary Report of Internal Audit. Vendor will on a regular basis audit the security of the systems that Process Personal Data. Upon FactSet's written requests, Vendor will make available to FactSet (or FactSet's independent, third-party auditor) a summary of the results of this audit ("Summary Report") to demonstrate compliance with the obligations under the Agreement. In the event such report and certifications are

deemed not to satisfy the requirements of the Agreement, FactSet may request an on-site audit relevant to the protection of Personal Data once every twelve-month period. FactSet shall promptly notify Vendor with information regarding any non-compliance discovered during the course of an audit.

- b. Cost. The cost of an audit on Vendor's premises will be borne by FactSet, unless: (i) Vendor committed a Material Breach (as defined in the Agreement and this VDPA) of the Agreement or any breach of this VDPA; or (ii) Vendor is out of compliance with Vendor's obligations under this VDPA, in which case Vendor will bear the costs.

6.4 Standard Contractual Clauses. To the extent that Standard Contractual Clauses are relied upon as the data transfer mechanism and the Processing of Shared Data involves a Restricted Transfer under the:

- i. GDPR, Vendor shall comply with its obligations as set out in module two of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council adopted by European Commission decision of 4 June 2021 and published under document number C/2021/3972 (the "EU C2P Standard Contractual Clauses" or "EU SCCs") and incorporated herein by reference. Any future updates or revisions to the EU SCCs by the European Commission are incorporated into this VDPA.
- ii. UK GDPR, Vendor shall comply with its obligations as set out in module two of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council adopted by European Commission decision of 4 June 2021 and published under document number C/2021/3972, as amended by the UK Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018 (the "UK C2P Standard Contractual Clauses" or "UK SCCs") and incorporated herein by reference. Any updates or revisions to the EU SCCs by the European Commission are incorporated into this VDPA.

6.5 If SCCs are relied upon as the applicable data transfer mechanism for this agreement, the current SCCs published by the EU Commission and Annexes I, II, and III are incorporated into this VDPA.

6.6 The Parties agree that, for the purposes of the EU C2P Standard Contractual Clauses and the UK C2P Standard Contractual Clauses:

- i. the optional clause set out at Clause 7 ('Docking clause') shall not apply;
- ii. the optional clause set out at Clause 11(a) ('Redress') shall not apply;
- iii. (for the EU C2P Standard Contractual Clauses only) for the purposes of Clause 13(a) ('Supervision') I, Option [2] shall apply and the competent Supervisory Authority shall be the Commissioner for Data Protection and Freedom of Information in the State of Hessen, Federal Republic of Germany;
- iv. (for the UK C2P Standard Contractual Clauses only) for the purposes of Clause 13(a) ('Supervision') I, Option [2] shall apply and the competent Supervisory Authority shall be the UK Information Commissioner's Office (ICO);
- v. (for the EU C2P Standard Contractual Clauses only) for the purposes of Clauses 17 ('Governing law') and 18(b) ('Choice of forum and jurisdiction') the governing law and jurisdiction shall be that of Germany;

- vi. (for the UK C2P Standard Contractual Clauses only) for the purposes of Clauses 17 ('Governing law') and 18(b) ('Choice of forum and jurisdiction') the governing law and jurisdiction shall be the Courts of England and Wales;
- vii. where a Restricted Transfer occurs, the data exporter shall be the Party effecting the Restricted Transfer of the Shared Data and the data importer shall be the Party in receipt of transferred Shared Data.

6.7 Vendor shall notify FactSet if it determines it can no longer meet obligations under Data Protection Law. Vendor acknowledges that FactSet has the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of FactSet Personal Data.

7. FAILURE TO COMPLY

7.1 Material Breach. Vendor's failure to comply with any of the provisions of this VDPA shall be deemed a Material Breach of the Agreement, and FactSet may terminate the Agreement without liability to Vendor if Vendor does not cure such breach (if capable of being cured) within ten (10) days of receipt of written notice of such breach from FactSet. FactSet may require Vendor to suspend Processing of Personal Data during this ten-day period pending such cure.

8. DATA SUBJECT RIGHTS

8.1 Vendor will, to the extent not legally prohibited, notify FactSet without undue delay within 72 hours of Vendor receiving a request from a Data Subject about the Personal Data of a Data Subject including but not limited to exercising the Data Subject's rights set forth in Data Protection Laws, including Chapter III of GDPR ("**Data Subject Request**"). Taking into account the nature of the Processing, Vendor will assist FactSet as requested in connection with the fulfilment of such Data Subject Request, including without limitation FactSet's obligation to respond to Data Subject Requests under Data Protection Laws. For clarity, Vendor will upon FactSet's request provide commercially reasonable efforts to assist FactSet in responding to such Data Subject Request.

9. RETURN AND DELETION OF PERSONAL DATA

9.1 Upon FactSet's request to Vendor's email address as defined in Annex I, Vendor will return or delete Personal Data in a manner specified by FactSet, unless and to the extent Data Protection Laws or the laws of EU member or U.S. states requires that Vendor retain the Personal Data. Vendor will delete Personal Data 30 days after termination or expiration of the Agreement, unless otherwise requested by FactSet. Vendor shall dispose of Personal Data in accordance with this Agreement, using standard(s) of data sanitization such as NIST 800-88 ("Guidelines for Media Sanitization") and ISO 27000 ("A.11.2.7 - Secure Disposal or Reuse of Equipment Control").

9.2 Once Personal Data is no longer required for Vendor to perform Vendor's obligations under the Agreement or this VDPA, Vendor shall immediately delete or securely return, at FactSet's discretion, Personal Data.

9.3 If FactSet provides Personal Data on a hard drive or other forms of removable media, such removable media must be encrypted, or password protected. In collaboration with FactSet, Vendor shall either return the removable media to FactSet, or securely destroy such removable

media by using a certified third-party. A Certificate of Destruction should be made available to FactSet upon request.

10. ENTIRE AGREEMENT, HIERARCHY.

- 10.1** If there is a conflict between the Agreement and this VDPA, the terms of this VDPA will take precedence to the extent of such conflict.
- 10.2** With respect to the processing of Personal Data subject to Data Protection Laws, in the event of any conflict or inconsistency between the terms of the Agreement or of this VDPA, the VDPA will control.

11. TERM AND TERMINATION

- 11.1** This VDPA shall enter into force at the same time as the Agreement and shall automatically terminate upon any termination or expiration of the Agreement.

12. MISCELLANEOUS

- 12.1 Additional Parties.** The parties agree that any Affiliates of FactSet may use the Services pursuant to the Agreement and this VDPA. All Affiliates of FactSet hereunder who use the Services pursuant to the Agreement are third-party beneficiaries of this VDPA and may bring any legal action, suit, claim or proceeding as if it were a party to this VDPA.
- 12.2 Liability Relief.** In no event will this VDPA or the Agreement relieve the parties from any liabilities imposed by applicable Data Protection Laws.
- 12.3 Governing Law.** Interpretation of this VDPA is governed by the law of the jurisdiction established in the main Agreement.
- 12.4 Severability.** If any provision of this VDPA is deemed unenforceable, such provision will be deemed modified to the least extent necessary to render it enforceable and such provision, taken with all other provisions hereof, will continue in full force and effect.
- 12.5 No Waiver.** The waiver by any party hereunder shall not be deemed to be nor construed as a further or continuing waiver. The failure of either party to enforce any right or provision of this VDPA shall not constitute a waiver of future enforcement of that right or provision.

13. APPLICATION OF CCPA

- 13.1** If the scope of Processing involves personal data of California employees or California Business contact information subject to the CCPA, the following shall additionally apply:
 - i. **“Business”** has the meaning set forth in the CCPA.
 - ii. **“Processor”** means the entity which Processes Personal Data on behalf of the Controller, including as applicable any **“Service Provider”** as that term is defined by the CCPA.

- iii. **“Service Provider”** means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert that processes personal information on behalf of a business and that receives from or on behalf of the business consumer’s personal information for a business purpose pursuant to a written contract.
- iv. **Share, Shared or Sharing”** means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data for purposes of cross-context behavioral advertising, whether or not for monetary or other valuable consideration.
- v. Vendor shall provide the same level of privacy protection for FactSet Personal Data as required of a Business under the CCPA.