Bloomberg Industry Group
1801 S. Bell Street
Arlington, VA 22202

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("Addendum") forms part of the Agreement between Customer and its affiliates covered under the Agreement, if any ("Data Controller", "Data Exporter" and "Customer") and BLOOMBERG INDUSTRY GROUP, INC. ("Data Processor", "Data Importer" and "Bloomberg Industry Group"), each a "Party" and collectively the "Parties", for the use of the Services (as defined herein) within the Bloomberg Tax Research product, to reflect the Parties' agreement concerning the processing of Protected Data for the Term specified in the Agreement.

This Addendum forms part of the terms for your use of the Bloomberg Tax Research product and services.

The terms of the Addendum govern how we comply with Data Protection Law in relation to the Protected Data described in Appendix 1 to Schedule 1 below.

This Addendum supplements and does not replace the Agreement. In the event of a conflict between the terms of this Addendum and the terms of the Agreement, the relevant terms of this Addendum shall apply. All capitalized terms that are not defined in this Addendum shall have the meaning set forth in the Agreement.
This Addendum excludes personal data for which Bloomberg Industry Group, Inc. is a Data Controller.

DEFINITIONS

In this Addendum:

A. **"Applicable Law"** means as applicable and binding on the Parties:
   (i) any law, statute, regulation, by-law or subordinate legislation in force from time to time to which a Party is subject;
   (ii) the common law and laws of equity as applicable to the Parties from time to time;
   (iii) any binding court order, judgment or decree; or
   (iv) any applicable direction, policy, rule or order that is binding on a Party and that is made or given by any regulatory body having jurisdiction over a Party or any of that Party's assets, resources or business;
B. **"Agreement"** means the terms governing the Bloomberg Industry Group Customer Agreement & any applicable Order Forms;
C. **"Binding Corporate Rules"** shall have the meaning given to that term in Regulation (EU) 2016/679 of the European Parliament and of the Counsel 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 ("**GDPR**");
D. **Business"** has the meaning set forth in Section 1798.140(c) of the CCPA or, effective January 1, 2023, Section 1798.140(d) of the CPRA.
E. **"Data Protection Laws"** means as applicable and binding on the Parties all laws, including, but not limited to, laws of the European Union ("EU"), the European Economic Area ("EEA"), Switzerland and the United Kingdom, the California Consumer Privacy Act of 2018 ("CCPA"); effective January 1, 2023, the California Privacy Rights Act (including its regulations) ("CPRA"), applicable to the processing of Protected Data under the Agreement and as amended from time to time;
F. **"Data Subject"** means the individuals whose Protected Data is governed by the Data Protection Laws and processed during the provision of the Services pursuant to this Addendum;
G. **"Data Subject Request"** means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;
H. **"Member State"** means EU Member State;
I. **"Personal Data"** has the meaning given to the term "personal data" or "personal information" in Data Protection Laws;
J. **"Processing"** has the meaning given to that term in Data Protection Laws (and related terms such as **process** have corresponding meanings);
K. **"Protected Data Breach"** means any breach of security leading to, the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Protected Data unless such breach is unlikely to result in a risk to the rights and freedoms of natural persons;

L. **"Protected Data"** means Personal Data provided by the Data Controller to the Data Processor about Data Subjects in connection with the performance of the Data Processor's obligations under the Agreement, as set out in Appendix 1 to Schedule 1;
M. **"Services"** means the processing of the Protected Data in the provision of Compliance Tracker, Document Upload, and any future product functionalities in which Data Processor is processing personal data on behalf of the Data Controller within Bloomberg Tax Research;
N. **"Service Provider"** has the meaning set forth in in Section 1798.140(v) of the CCPA or, effective January 1, 2023, Section 1798.140(ag)(1) of the CPRA.
O. **Standard Contractual Clauses"** means Standard Contractual Clauses for the transfer of EU Protected Data to third countries pursuant to the GDPR and approved European Commission Implementing Decision (EU) 2021/914 of 4 June 2021;
P. **"Sub-Processor"** means another Data Processor engaged by the Data Processor for carrying out processing activities in respect of the Protected Data on behalf of the Data Controller;
Q. **"Supervisory Authority"** means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;
R. **"Third Country"** means a country outside the UK, EEA or Switzerland which has not been deemed adequate to receive Protected Data under the Data Protection Laws of the country of the party transferring Protected Data.

DATA PROCESSING PROVISIONS

1. DATA CONTROLLER OBLIGATIONS

1.1 The Data Controller shall comply with all Data Protection Laws in connection with the processing of Protected Data, the Services and the exercise and performance of its respective rights and obligations under this Addendum, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws.

1.2 The Data Controller warrants, represents and undertakes, that:

1.2.1 all Protected Data sourced or provided by the Data Controller for use in connection with the Services, shall comply in all respects, including in terms of its collection, storage and processing, with Data Protection Laws; and

1.2.2 all instructions given by the Data Controller to the Data Processor in respect of Protected Data shall at all times be in accordance with Data Protection Laws.

2. **INSTRUCTIONS AND DETAILS OF PROCESSING**

2.1 Insofar as the Data Processor processes Protected Data on behalf of the Data Controller, the Data Processor:

2.1.1 unless required to do otherwise by Applicable Law or Data Protection Laws, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Data Controller's instructions in connection with the provision of the Services;

2.1.2 if Applicable Law requires it to process Protected Data other than in accordance with the Data Controller's instructions, shall notify the Data Controller of any such requirement before processing the Protected Data (unless Applicable Law prohibits such notification); and

2.1.3 shall inform the Data Controller if the Data Processor becomes aware of a Data Controller instruction that, in the Data Processor's opinion, infringes Data Protection Laws, provided that this shall be without prejudice to clauses 2.1.1 and 2.1.2. The Data Processor shall, without liability, be entitled to cease any processing of Personal Data affected by such infringing instruction.

2.2 The parties agree that, for the purposes of the Protected Data, the Data Controller is a Business, and the Data Processor is a Service Provider. The Data Controller hereby instructs the Data Processor to Process Protected Data solely to the extent necessary to provide the Services to and on behalf of the Data Controller. The Data Processor is not entitled to Process Protected Data for its own purposes including, without limitation, sharing Protected Data with third parties (other than approved Subprocessors).

2.3 The Data Controller discloses or otherwise makes available Protected Data to the Data Processor for the limited and specific purpose of the Data Processor providing the Services to the Data Controller. The Data Processor shall: (i) comply with all applicable obligations under the CPRA; (ii) provide the same level of protection as required of a Business under the CPRA; (iii) notify the Data Controller if it can no longer meet its obligations under the CPRA; (iv) not "sell" or "share" (as such terms are defined by the CCPA and/or the CPRA) Protected Data; (v) not retain, use, or disclose Protected Data for any purpose (including, but not limited to, any commercial purpose) other than to provide the Services under the Agreement; (vi) not retain, use, or disclose Protected Data outside of the direct business relationship between the Data Controller and the Data Processor; and (vii) if and to the extent inconsistent with the limitations on Service Providers under the CCPA and/or CPRA, not combine Protected Data with Personal Data that the Data Processor (1) receives from, or on behalf of, another person or (2) collects from its own, independent consumer interaction. The Data Controller may: (a) to take reasonable and appropriate steps to help ensure that the Data Processor Processes Protected Data in a manner consistent with the Data Controller's CPRA obligations; and (b) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized Processing of Protected Data by the Data Processor.

3. **TECHNICAL AND ORGANISATIONAL MEASURES**

3.1.1 The Data Processor shall, taking into account the state-of-the-art, the costs of implementation and the nature of the processing as well as a level of security appropriate to the risk to the rights and freedoms of Data Subjects, implement and maintain appropriate technical and organizational measures against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Protected Data, as described below:

3.1.2 measures in relation to the processing of Protected Data by the Data Processor, as set out in Appendix 2 to Schedule 1 (Technical and organisational measures) of this Addendum and

3.1.3 measures required to assist the Data Controller insofar as is possible in the fulfilment of the Data Controller's obligations to respond to Data Subject Requests relating to Protected Data.

3.1.4 Notwithstanding any provision to the contrary, the Data Processor may modify or update these measures at its discretion provided that such modification or update does not result in a material degradation in the protection offered by the technical and organisational measures.

4. **USING STAFF AND OTHER PROCESSORS**

4.1 Subject to Clause 4.2, the Data Controller authorizes the engagement of Sub-Processors for the purpose of carrying out any processing activities in respect of the Protected Data. The Data Processor shall notify the Data Controller of any addition or replacement of the Sub-Processors as set out in the Standard Contractual Clauses in Schedule 1. The Data Controller may notify the Data Processor within thirty (30) days of any reasoned objection to any such addition or replacement on the basis that such addition or replacement causes the Data Controller to violate Applicable Law (a "Valid Objection"). In the event of a Valid Objection, the Data Controller shall have an additional right to terminate the Agreement, on written notice provided within 30 days from the date the Data Processor notifies the Data Controller of any addition or replacement of the Sub-Processors and pursuant to Section 10 of the Agreement, in the event that the Data Processor engages the Sub-Processor after a Valid Objection has been made. For the avoidance of doubt, all other terms and conditions contained in the Agreement shall remain unchanged.

4.2 The Data Processor shall only appoint Sub-Processors under a written contract containing materially the same obligations to those set out under Sections 1 to 9 (inclusive) of this Addendum.

4.3 The Data Processor shall remain fully responsible to the Data Controller for the performance of the Sub-Processor's obligation in accordance with the contract with the Sub-Processor.

4.4 The Data Processor shall ensure that all Data Processor personnel authorised to process Protected Data are subject to a binding written contractual obligation with the Data Processor to keep the Protected Data confidential (except where disclosure is permitted under Applicable Law, in which case the Data Processor shall, where practicable and not prohibited by Applicable Law, notify the Data Controller of any such requirement before such disclosure or as otherwise contemplated under the Agreement).

5. **ASSISTANCE WITH THE DATA CONTROLLER'S COMPLIANCE AND DATA SUBJECT RIGHTS**

5.1 The Data Processor shall refer all Data Subject Requests it receives to the Data Controller within a reasonable period of time of receipt of the request, provided that if the number of Data Subject Requests exceeds 2 per calendar month, the Data Controller shall pay the Data Processor's reasonable expenses for recording and referring the Data Subject Requests in accordance with this clause.

5.2 The Data Processor shall provide such reasonable assistance as the Data Controller reasonably requires (taking into account the nature of processing and the information available to the Data Processor and to the extent that the Controller does not otherwise have access to the required information) to the Data Controller in connection with the Services, in ensuring compliance with the Data Controller's obligations under Data Protection Laws with respect to:

5.2.1 data protection impact assessments (as such term is defined in Data Protection Laws), at the Data Controller's cost;

5.2.2 prior consultation with a Supervisory Authority regarding high risk processing and general cooperation with the Supervisory Authority in the performance of its tasks; and

5.2.3 notifications to the Supervisory Authority and/or communications to Data Subjects by the Data Controller in response to any Protected Data Breach.

6. INTERNATIONAL DATA TRANSFERS

6.1 The Data Controller agrees that the Protected Data shall be transferred to the Data Processor and its Sub-Processors, which may be located in a Third Country. The Parties agree:

6.1.1 where the Data Controller is in the EEA and transfers Protected Data to the Data Processor in a Third Country, to comply with their respective obligations under the Standard Contractual Clauses, Module Two, as set out in Schedule 1 (EEA data transfers);

6.1.2 where the Data Controller is in the UK or Switzerland and transfer of Protected Data to the Data Processor in a Third Country, to comply with their respective obligations under Schedule 2 (UK and Swiss data transfers); or

6.1.3 that transfers from the Data Controller to the Data Processor may be made under any other compliant transfer mechanism approved under the relevant Data Protection Laws, including Binding Corporate Rules or any successor to the EU-US Privacy Shield.

6.2 The provisions of this Addendum shall constitute the Data Controller's instructions with respect to transfers in accordance with clause 2.1.

7. RECORDS, INFORMATION AND AUDIT

7.1 The Data Processor shall maintain, in accordance with Data Protection Laws binding on the Data Processor, written records of all categories of processing activities of the Protected Data carried out on behalf of the Data Controller.

7.2 The Data Processor shall provide, upon the Data Controller's request, all information reasonably necessary to demonstrate the Data Processor's compliance with this Addendum.

7.3 If the Data Controller has justifiable reason to believe that the Data Processor is not complying with the terms and conditions under the Addendum, in particular with the obligation to maintain and implement the agreed technical and organizational measures, or those arising out of inquiries by its auditors or regulators, the Data Processor will use commercially reasonable efforts to work in good faith to respond to further inquiries by Data Controller (including Data Controller inquiries arising out of inquiries by its auditors or regulators) regarding Data Processor's information security program as it relates to Protected Data, which may include (1) an onsite visit of Data Processor's offices at 1801 S. Bell Street Arlington, VA 22202 no more than once per calendar year, at a mutually agreed upon time during Data Processor's normal business hours and (2) no more than once every calendar year, requiring Data Processor to complete or respond to a risk due diligence document provided by Data Controller requesting information on information security and related measures. During the course of any onsite visit by Data Controller, Data Processor shall make available to Data Controller (i) information pertaining to Data Processor's information security program as it relates to Protected Data, (ii) appropriate

personnel to review with Data Controller such information security program and (iii) other information related to compliance with the Agreement and this Addendum as requested by Data Controller and reasonably available to the Data Processor. Any onsite visit shall be subject to Data Processor's standard security and confidentiality procedures and practices, including but not limited to, Data Processor's requirement that Data Controller must enter into a non-disclosure agreement before the visit. In addition, Data Processor shall provide Data Controller with the following information: (x) updates on internal security measures (y) risk reports (e.g. SOC reviews, where available), penetration assessment summaries and due diligence documentation, and (z) selected risk and compliance information and evidence of its internal security controls through additional on-site visits, questionnaires, phone calls and video conference meetings, in each case to the extent Data Processor deems the provision of such information to be appropriate in its sole good faith discretion and makes such information generally available to similarly situated customers of Data Processor.

8. **BREACH NOTIFICATION**

8.1 In respect of any actual Protected Data Breach, the Data Processor shall, without undue delay:
8.1.1 notify the Data Controller of the Protected Data Breach; and
8.1.2 provide the Data Controller with details of the Protected Data Breach.

9. **DELETION OR RETURN OF PROTECTED DATA AND COPIES**

9.1 The Data Processor shall delete or return all the Protected Data to the Data Controller in accordance with the terms of the Agreement unless prohibited by Applicable Law.

10. **LIABILITY, INDEMNITIES AND COMPENSATION CLAIMS**

10.1 To the maximum extent permitted by law and without amending the Standard Contractual Clauses set out in Schedule 1 or the liability provisions in the Agreement, the Data Processor shall not be liable for any breaches of this Addendum except for direct actual data protection losses (losses incurred by, awarded against or agreed to be paid by the Data Controller arising under or in connection with this Addendum ("Data Protection Losses")) that are both (x) caused by the Data Processor's processing of Protected Data under this Addendum and (y) directly resulting from the Data Processor's or the Data Processor's Sub-Processors' breach of this Addendum. To the maximum extent permitted by law, Data Processor shall not be liable for any consequential or indirect Data Protection Losses contributed to or caused by any breach of this Addendum or the Agreement by the Data Controller or otherwise caused by the acts or omissions of the Data Controller.

10.2 Notwithstanding the foregoing, to the maximum extent permitted by law, Data Processor's aggregate liability to a Data Controller for Data Protection Losses regardless of the form of the action, shall in no event exceed $10,000.

10.3 No party shall be liable to the other for any default resulting from force majeure, which shall be deemed to include any circumstances beyond the reasonable control of the party or parties affected. Except to the extent expressly provided in Schedule 1, the Data Processor and its affiliates shall not be liable for any claim or demand against Data Controller by a third party.

11. **TERMINATION**

11.1 *Termination of Agreement.* This Addendum ends automatically when the termination or expiration of all Services provided under the Agreement becomes effective.

12. **MISCELLANEOUS**

12.1 *Governing law.* This Addendum will be governed by and interpreted in accordance with the laws of England & Wales. This provision does not amend the governing law provision in the Agreement.

12.2 *Entire contract.* Together with the Agreement, this Addendum constitutes the entire contract of the Parties, and supersedes any previous contracts whether oral or in writing between the Parties with regard to the subject matter of this Addendum.

12.3 *Severability.* The validity of this Addendum will not be affected if any section of, or annex to, this Addendum (or part thereof) is invalid or otherwise unenforceable. Instead of the invalid or unenforceable provision, the Parties shall negotiate on an arrangement which comes as close as legally possible to what the Parties were trying to achieve with the invalid or unenforceable provision (or, as the case may be, the invalid or unenforceable part thereof). The same shall apply if this Addendum contains a gap or omission.

12.4 *Variations.* Data Processor may update this Addendum at this URL from time to time by posting an updated Addendum on this URL, and Data Controller's continued use of the Product constitutes its acceptance of the updated Addendum.

SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Transfer controller to processor SECTION I

Cause 1 - Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:
   (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
   (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')
   (iii) have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2- Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8.1 (b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e)
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e); (viii)Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4- Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5-Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.Clause 7 – Optional Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Clause 7 – Optional Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8- Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The

Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub- processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

processor to erase or return the personal data.

Clause 10 - Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 - Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

    (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
    (ii) refer the dispute to the competent courts within the meaning of Clause 18

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

MODULE TWO: Transfer controller to processor

Clause 12- Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject

shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its subprocessor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13- Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14- Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];
(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15- Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16- Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
    (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
    (ii) the data importer is in substantial or persistent breach of these Clauses; or
    (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority

regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such noncompliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or
(ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

MODULE TWO: Transfer controller to processor

Clause 17- Governing Law

These Clauses shall be governed by the law of one of the EU Member States in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for such third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands.

MODULE TWO: Transfer controller to processor

Clause 18- Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of The Netherlands.
(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Appendix

Annex I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data Exporter(s):
The Data Exporter is the Data Controller. The Data Controller will obtain the Services from the Data Importer as described below in accordance with the Agreement.

Data Importer(s):
The Data Importer is Bloomberg Industry Group, Inc. ("Data Processor"). The Data Processor will provide the Data Controller with the Services described below in accordance with the Agreement.

B. **DESCRIPTION OF TRANSFER**

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

The personal data transferred concern the following categories of data subjects:

Data Subjects include any persons whose Personal Data may be uploaded by Data Exporter users via the Services (e.g., current and former clients of the Data Exporter).

Categories of personal data transferred

Personal data, including, but not limited to, names and contact details that are provided by the Data Exporter to Data Importer for purposes of providing the Services.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Sensitive personal data may be uploaded by the Data Exporter to Data Importer for the purposes of providing the Services.

For restrictions and safeguards, see Annex II, Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous, unless otherwise set forth in the Agreement.

Nature of the processing

The Data Importer will input, maintain, process, and store the Data Exporter's Personal Data included in the records which will include the categories of data set out above, for purposes of providing the Services.

Purpose(s) of the data transfer and further processing

The purpose of the data transfer and any further processing of Personal Data by the Data Importer is to provide the Services pursuant to the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal Data will be retained by the Data Importer for the period set forth in the Agreement.

For transfers to sub-processors, also specific subject matter, nature and duration of processing

The subject matter and nature of the processing will further the Data Importer's purpose of providing the Services pursuant to the Agreement. The duration of the processing will not exceed what is required for the sub-processor to perform its sub-processing activities, which is not to exceed the period for which the Data Importer may retain the Personal Data described in this Addendum.

C. **COMPETENT SUPERVISORY AUTHORITY**

MODULE TWO: Transfer controller to processor

The competent supervisory authority specified in accordance with Clause 13.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

Data Importer will maintain and enforce physical and logical security procedures with respect to its access and maintenance of personal data contained on Data Importer servers.

Data Importer will use reasonable measures to secure and defend its location and Services against "hackers" and others who may seek to modify or access the Data Importer servers or the information found therein without authorization. Data Importer will test its systems for potential security breaches and vulnerabilities at least annually.

Data Importer has a written information security program ("Information Security Program") that includes administrative, technical, and physical safeguards that protect against any reasonably anticipated threats or hazards to the confidentiality of the personal data, and protect against unauthorized access, use, disclosure, alteration, or destruction of the personal data. In particular, the Data Importer's Information Security Program shall include, but not be limited, to the following safeguards where appropriate or necessary to ensure the protection of personal data:

Access Controls – policies, procedures, and physical and technical controls: (i) to limit physical access to its information systems and the facility or facilities in which they are housed to properly authorized persons and (ii) to authenticate and permit access only to authorized individuals. Access controls at Data Importer are based on the principle of "least privilege," whereby authorized users are only granted access to information systems, networks and data as necessary to carry out their roles and responsibilities. No access is granted beyond that which is required for a user to fulfill his or her responsibilities.

Security Incident Procedures – policies and procedures to detect, respond to, and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into personal data or information systems relating thereto, and procedures to identify and respond to validated security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes.

Data Importer monitors changes to roles, titles and business requirements in order to correctly and quickly maintain a least-privilege approach to data access across the organization.

Device and Media Controls – policies and procedures that govern the receipt and removal of hardware and electronic media that contain personal data into and out of a Data Importer data center, and the movement of these items within a Data Importer data center, including policies and procedures to address the final disposition personal data.

Event Logging – hardware, software, and/or procedural mechanisms that record activity in information systems that contain or use personal data and review such activity in the event of an anomaly. Procedures are in place governing configuration of systems and applications to generate audit logs, including security event logs. The procedures detail what type of information should and should not be logged and what security controls should be applied.

Data Integrity – policies and procedures to guard against the unauthorized disclosure, improper alteration, or unauthorized destruction of personal data.

Encryption and Transmission Security – Data Importer offers support to provide encryption of electronic information while in transit to guard against unauthorized access to personal data that is being transmitted over public communications network. Data Importer supports the encryption of communication channels for data in motion and data at rest.

Network Security - Data importer maintains network security using commercially available equipment and industry standard techniques, including firewalls, intrusion detection and prevention systems, access control lists and routing protocols.

Secure Disposal – policies and procedures regarding the disposal of personal data, taking into account available technology that can be used to sanitize storage media such that stored data cannot be practicably read or reconstructed. Data is retained according to Data Importer's published policy and/or legal and regulatory requirements.

Testing – Data Importer shall regularly test the key controls, systems and procedures of its Information Security Program to verify that they are properly implemented and effective in addressing the threats and risks identified in accordance with our policy

Adjust the Program – Data Importer shall monitor, evaluate, and adjust, as it deems necessary, the Information Security Program in light of any relevant changes in technology or industry security standards, the sensitivity of, and internal or external threats to Data Importer or the personal data.

Security Training – Data Importer shall provide annual security awareness and data privacy training for its employees that will have access to personal data.

Separation of Data – Data Importer uses technical capabilities such as logical access separation to achieve data separation

Human Resources Security – Data Importer's policies require that any new employees undergo, upon hire and prior to being granted access to personal data, a background check, where lawfully permitted, and enter into a confidentiality agreement, consistent with the confidentiality obligations of Data Importer under the Agreement and this Addendum that are applicable to the work performed by such employees.

Business Continuity and Disaster Recovery - Data Importer shall maintain policies and procedures to ensure that Data Importer may continue to perform business critical functions in the face of an extraordinary event. This includes data center resiliency and disaster recovery procedures for business-critical data and processing functions.

For transfers to sub-processors, the Data Importer shall ensure the sub-processor maintains administrative, physical, organizational, and technical safeguards that are at least as protective of the personal data as those required to be taken by the Data Importer pursuant to the Agreement and these Standard Contractual Clauses.

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorization of sub-processors (Clause 9(a), Option 1).

The subprocessors listed on Bloomberg Industry Group's Trust Center.

SCHEDULE 2

TRANSFER MECHANISM FOR DATA TRANSFERS FROM THE UK OR SWITZERLAND

In case of any transfers of Protected Data from the United Kingdom or Switzerland, the Standard Contractual Clauses in Schedule 1 are hereby incorporated and amended as necessary as set out in this Schedule 2:

For data transfers from the UK:

The International Data Transfer Addendum ("IDTA") issued by the UK Information Commissioner's Office, version B1.0 having effect from 21 March 2022 is hereby incorporated.

Part 1: Tables

Table 1: Parties

As set out in the Agreement.

Table 2: Selected SCCs, Modules and Selected Clauses

The version of the Approved EU SCCs included in Schedule 1, including the appendix information.

Table 3: Appendix Information

Annex 1A: List of Parties: Parties are set out in Table 1 above
Annex 1B: Description of Transfer: Refer to Schedule 1 above
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Refer to Schedule 1 above
Annex III: List of Sub processors (Modules 2 and 3 only): Refer to Schedule 1 above.

Table 4: Ending the IDTA when it changes *Neither party may end this IDTA.* Alternative Part 2 Mandatory Clauses:

Part 2: Mandatory Clauses of the IDTA, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

For data transfers subject to the Swiss Federal Act on Data Protection ("Swiss DPA"):

In respect of data transfers subject to the Swiss DPA, the Standard Contractual Clauses shall apply with the following amendments (these amendments shall not affect the application of the Standard Contractual Clauses for the purposes of other applicable Data Protection Laws):

- In Clause 2, delete the words: "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";
- Clause 6 is replaced with: "The details of the transfer(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred are those specified in Annex I.B where the Swiss DPA applies to the data exporter's processing when making that transfer.";
- Clause 8.8(i) of Module Two is replaced with: "the onward transfer is to a country that has been the subject

of an adequacy assessment by the Federal Data Protection and Information Commissioner ("**FDPIC**") or the Federal Council (as the case may be) that covers the onward transfer";

- References to "Regulation (EU) 2016/679", "Regulation (EU) 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 (General Data Protection Regulation)" and "that Regulation" are to be interpreted as references to the Swiss DPA to the extent applicable;
- References to "Regulation (EU) 2018/1725" are removed;
- References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" shall be interpreted to mean Switzerland;
- Clause 13 (a) and Part C of Annex I are not used;
- The "competent supervisory authority" and "supervisory authority" are both replaced with the FDPIC insofar as the data transfers are governed by the Swiss DPA;
- In Clause 16(e), subsection (i) is replaced with: "the FDPIC adopts its own standard contractual clauses pursuant to Article 16(2)(d) of the Swiss revised DPA that cover the transfer of personal data to which these clauses apply";
- Clause 17 is replaced with: "These Clauses are governed by the laws of Switzerland insofar as the data transfers are governed by the Swiss DPA.";
- Clause 18 is replaced with: "Any dispute arising from these Clauses relating to the Swiss DPA shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The parties agree to submit themselves to the jurisdiction of such courts."; and

- As long as the Swiss DPA of 19 June 1992 is in force, the Standard Contractual Clauses shall also protect Personal Data of legal entities and legal entities shall receive the same protection under the Standard Contractual Clauses as natural persons.