Data Protection Agreement

Amendment **to [insert name agreement, contract, ordering documents or any other written agreement]** (“**Agreement**”)

1. SCOPE, ORDER OF PRECEDENCE, AND TERM

1.1. This Data Processing Agreement (“**DPA**”) is between Customer and its Affiliates (collectively, “**Customer**”), and the signatory to this DPA, Virtru Corporation (“**Virtru**”). By signing the DPA, Virtru enters into this DPA on behalf of itself and its Affiliates.

1.2. This DPA is part of any and all agreements, purchase orders, statements of work and other contractual documents between Customer and Virtru (individually and collectively, the “**Agreement**”). Customer and Virtru are individually a “**party**” and, collectively, the “**parties**.”

1.3. The effective date of the DPA is the date of the Agreement, or the date that Customer first begins using the Virtru Services (as “**Virtru Services**” are defined in the Agreement), whichever is earlier.

1.4. This DPA applies only to the extent that Virtru receives, stores, or Processes Personal Data in connection with the Virtru Services.

1.5. In the event of a conflict between this DPA and the Agreement, the DPA will control to the extent necessary to resolve the conflict. In the event the parties use an International Data Transfer Mechanism and there is a conflict between the obligations in that International Data Transfer Mechanism and this DPA, the International Data Transfer Mechanism will control except as specified in this DPA.

1.6. The term of this DPA is coterminous with the Agreement, except for obligations that survive past termination as specified below.

2. DEFINITIONS

2.1. The following terms have the meanings set forth below. All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement.

2.2. The following terms have the definitions given to them in the CCPA: “**Business**,” “**Sale**,” “**Service Provider**,” and “**Third Party**.”

2.3. “**Controller**” means the entity that determines the purposes and means of the Processing of Personal Data. “Controller” includes equivalent terms in other Data Protection Law, such as the CCPA-defined term “Business” or “Third Party,” as context requires.

2.4. “**Data Protection Law**” means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement, including Regulation 2016/679 (General Data Protection Regulation) (“**GDPR**”), and Cal. Civ. Code Title 1.81.5, § 1798.100 et seq. (California Consumer Privacy Act) (“**CCPA**”).

2.5. “**Data Subject**” means any identified or identifiable natural person about whom Personal Data may be Processed under this Amendment.

2.6. “**EEA**” means the European Economic Area.

2.7. “**Personal Data**” means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a Data Subject. “Personal Data” includes equivalent terms in other Data Protection Law, such as the CCPA-defined term “Personal Information,” as context requires.

2.8. "**Personal Data Breach**" means a confirmed breach of security of the Virtru Services that caused an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed by Virtru in the context of this Amendment.

2.9. "**Processing**" or "**Process**" means any operation or set of operation(s) performed upon Personal Data whether by automatic means or not, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of Personal Data.

2.10. "**Processor**" means an entity that processes Personal Data on behalf of another entity. "Processor" includes equivalent terms in other Data Protection Law, such as the CCPA-defined term "Service Provider," as context requires.

2.11. "**Sensitive Data**" means the data revealing a Data Subject's racial or ethnic origin; political opinions, religious or philosophical beliefs; trade union membership; genetic data; government identification numbers; biometric data; health data; sex life or sexual orientation; or criminal records.

2.12. "**Standard Contractual Clauses**" means the European Union standard contractual clauses for international transfers from the European Economic Area to third countries, Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

2.13. "**Subprocessor**" means a Processor engaged by a party who is acting as a Processor.

3. DESCRIPTION OF THE PARTIES' PERSONAL DATA PROCESSING ACTIVITIES AND STATUSES OF THE PARTIES

3.1. Annex I describes the purposes of the parties' Processing, the types or categories of Personal Data involved in the Processing, and the categories of Data Subjects affected by the Processing.

3.2. Annex I lists the parties' statuses under relevant Data Protection Law.

4. INTERNATIONAL DATA TRANSFER

4.1. Some jurisdictions require that an entity transferring Personal Data to, or accessing Personal Data from, a foreign jurisdiction take extra measures to ensure that the Personal Data has special protections (an "**International Data Transfer Mechanism**"). The parties will comply with any International Data Transfer Mechanism that may be required by applicable Data Protection Law, including the Standard Contractual Clauses. Virtru will protect Personal Data in accordance with this Amendment regardless of the jurisdiction in which it is located.

4.2. Before Customer transfers to Virtru or permits Virtru to access Personal Data located in a jurisdiction that requires an International Data Transfer Mechanism, Controller will notify Virtru of the relevant requirement and the parties will work together in good faith to fulfil the requirements of that International Data Transfer Mechanism. If the International Data Transfer Mechanism on which the parties rely is invalidated or superseded, the parties will work together in good faith to find a suitable alternative.

4.3. With respect to Personal Data of Data Subjects located in the EEA, Switzerland, or the United Kingdom that Customer transfers to Virtru or permits Virtru to access, the parties agree that by executing this DPA they also execute the Standard Contractual Clauses, which will be incorporated by reference at Exhibit A and form an integral part of this DPA. The parties agree that, with respect to the elements of the Standard Contractual Clauses that require the parties' input, Annexes I, II, and III contain all the relevant information. The parties agree that, for Personal Data of Data Subjects in the United Kingdom and Switzerland, they adopt the modifications to the Standard Contractual Clauses listed in Annex I to adapt the Standard Contractual Clauses to United Kingdom or Swiss law, as applicable.

5. DATA PROTECTION GENERALLY

5.1. Compliance. The parties will comply with their respective obligations under Data Protection Law and their privacy notices.

5.2. Cooperation:

5.2.1. Data Subject Requests or Complaints. Virtru will promptly notify Customer if Virtru receives: (i) any requests from a Data Subject with respect to Personal Data Processed by Virtru, including but not limited to opt-out requests, requests for access and/or rectification, blocking, erasure, requests for data portability, and all similar requests, and will not respond to any such requests unless expressly authorized to do so by Customer; or (ii) any complaint relating to the Processing by Virtru of Personal Data, including allegations that such Processing infringes on an Data Subject's rights. Customer is responsible for ensuring the accuracy of any Personal Data provided to Virtru.

5.2.2. Governmental and Investigatory Requests. If either party receives any type of request or inquiry from a governmental, legislative, judicial, law enforcement, or regulatory authority (e.g. the Federal Trade Commission, the Attorney General of a U.S. state, or a European data protection authority), or faces an actual or potential claim, inquiry, or complaint in connection with the parties' Processing of Personal Data (collectively, an "**Inquiry**"), the receiving party with notify the other party without undue delay unless such notification is prohibited by applicable law. If requested by the receiving party, the other party will provide the receiving party with information relevant to the Inquiry to enable the receiving party to respond to the Inquiry.

5.3. Confidentiality. The Parties will ensure that their employees, independent contractors, and agents are subject to an obligation to keep Personal Data confidential and have received training on data privacy and security that is commensurate with their responsibilities and the nature of the Personal Data.

6. DATA SECURITY

6.1. Security Controls. Virtru will implement reasonable technical and organizational safeguards designed to protect Personal Data against a Personal Data Breach. The safeguards will include the measures listed in Annex II of this DPA. Virtru may modify such safeguards from time to time, provided that such modifications will not materially reduce the overall level of protection for Personal Data. At Customer's request, Virtru will provide reasonable assistance to Customer in meeting its obligations under applicable data protection laws with respect to the security of the Processing of Personal Data through the Virtru Services, taking into account the nature of the Processing and the information available to Virtru. Virtru reserves the right to charge a reasonable fee to Customer for such requested assistance, to the extent permitted by applicable law.

7. VIRTRU'S OBLIGATIONS AS A PROCESSOR, SUBPROCESSOR, OR SERVICE PROVIDER

7.1. Virtru will have the obligations set forth in this Section 7 if it Processes the Personal Data of End Users in its capacity as Customer's Processor or Service Provider.

7.2. Scope of Processing: Virtru will Process Personal Data solely in accordance with the Agreement or other documented instructions of Customer (whether in written or electronic form), or as otherwise required by applicable law. Notwithstanding anything to the contrary, the parties agree that Virtru may, and Customer instructs Virtru to, Process Personal Data for the following activities that support the Virtru Services: detect data security incidents; protect against fraudulent or illegal activity; effectuate repairs; and build, improve, or maintain Virtru's products and services; provided that when it Processes Personal Data for these purposes, Virtru will use reasonable efforts to use pseudonymous or de-identified data and will not Process Personal Data it collects in connection with the Agreement for the commercial benefit of any third party.

7.3. Virtru's Subprocessors: Customer agrees that Virtru may use the Subprocessors listed in Annex III of the Standard Contractual Clauses. Customer agrees that Virtru may disclose Personal Data to its subcontractors for purposes of providing Virtru Services to Customer ("**Subprocessors**"), provided that Virtru will impose substantially similar obligations on its Subprocessors regarding the security and confidentiality of Personal Data as those set forth in this Amendment. Virtru will (a) maintain a list of its Subprocessors and will provide this list to Customer upon Customer's request and (b) provide Customer at least 30 days' prior notice of the addition of any Subprocessor to this list and the opportunity to object to such addition(s) on the grounds related to privacy and data protection issues. If Customer objects to such addition(s), Customer may elect to exercise any applicable termination right under the Agreement. Virtru will remain responsible for its Subprocessor's Processing activities in connection with the Agreement.

7.4. Personal Data Breach: In the event of a Personal Data Breach, Virtru will notify Customer without undue delay, unless otherwise prohibited by law or otherwise instructed by a law enforcement or supervisory authority. Following such notification, Virtru will provide reasonable assistance and cooperation requested by Customer. Customer agrees that Virtru may not notify Customer of a security-related event that does not result in a Personal Data Breach.

7.5. Audits

7.5.1. At Customer's written request, Virtru will assist Customer in the event of an investigation by a competent regulator, including a data protection regulator or similar authority, if and to the extent that such investigation relates to the Processing of Personal Data by Virtru on behalf of Customer in accordance with this Amendment (the "**Inspection**"). Virtru reserves the right to charge a reasonable fee to Customer for an Inspection, to the extent permitted by applicable law.

7.5.2. If an Inspection requires Customer to conduct an on-premise audit of Virtru, and if such Inspection is required by law applicable to Customer, Customer will provide Virtru with written notice at least 60 days in advance. Such written notice will specify the things, people, places, or documents to be made available and a citation to the legal authority that compelled Customer to request the Inspection. Such written notice, and anything produced in response to it (including any derivative work product such as notes of interviews), will be considered confidential information and will remain confidential information in perpetuity or the longest time allowable by applicable law after termination of the Agreement. Such materials and derivative work product produced in response to the Inspection will not be disclosed to anyone without the prior written permission of Virtru unless such disclosure is required by applicable law. If disclosure is required by applicable law, Customer will give Virtru prompt written notice of that requirement and an opportunity to obtain a protective order to prohibit or restrict such disclosure except to the extent such notice is prohibited by applicable law or order of a court or governmental agency. Customer agrees to negotiate in good faith with Virtru before seeking to exercise such audit or on-site inspection right more frequently than once per twelve (12) month period. Customer will make every effort to cooperate with Virtru to schedule the Inspection at a time that is convenient to Virtru. Customer agrees that if it uses a third party to conduct the Inspection, the third party will sign a non-disclosure agreement. Customer agrees that the Inspection will only concern Virtru's architecture, systems, policies, records of processing, data protection impact assessments, and procedures relevant to its obligations as set forth in the Agreement and the Processing of Personal Data carried out by Virtru and the Virtru Services as provided to Customer. Customer agrees that Virtru shall be allowed to protect or redact the names and identifying or proprietary information of other Virtru customers during the Inspection.

7.5.3. At least once per calendar year, Virtru will retain independent third-party auditors to prepare a Service Organization Controls 2, Type 2 report or comparable report ("**Report**"). Upon Customer's request, Virtru will provide to Customer a copy of the most recent Report, up to once per year. Such Reports will be Virtru Confidential Information under the confidentiality provisions of the Agreement .

7.6 Deletion. Upon termination or expiration of the Agreement for any reason, Virtru will return or destroy Personal Data at Customer's request, except as otherwise required by law applicable to Virtru. Annex I further describes Virtru's Personal Data retention policies.

[signatures]

Exhibit A

STANDARD CONTRACTUAL CLAUSES
Controller to Processor

SECTION I

Clause 1

PURPOSE AND SCOPE

(a) The purpose of these standard contractual clauses is to ensure compliance with therequirements 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) 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 AnnexI.A (hereinafter each 'data importer') 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.

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

(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

The parties do not permit docking.

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.

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 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 ithas 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 tothe 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 ofconfidentiality.

(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 (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 the onward transfer is necessary in order to protect the vital interests of the data subject or of another 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 non-compliance. 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

(a) 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 [*Specify time period*] 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 beneficiary rights for data subjects. 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-processor to erase or return the personal data.

Clause 10

DATA SUBJECT RIGHTS

(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.

(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.

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 sub-processor) 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) The supervisory authority with responsibility for ensuring compliance by the data exporterwith Regulation (EU) 2016/679 as regards the data transfer, 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

(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;

(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 ofdestination.

(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 theseClauses.

(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 hasbecome 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 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 MINIMISATION

(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 non-compliance. 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.

Clause 17

GOVERNING LAW

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of [governing jurisdiction is the Member State in which the data exporter is established].

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 [governing jurisdiction is the Member State in which the data exporter is established].

(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.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1.	Name:	[Insert details]
	Contact person's name, position and contact details:	[Insert details]
	Activities relevant to the data transferred under these Clauses:	Processing to carry out the Virtru Services pursuant to the Agreement entered into between Customer and Virtru Corporation.
	Signature and date:	This Annex I shall automatically be deemed executed when the Agreement is executed.
	Role (controller/processor):	Controller in relation to all Personal Data Processed in connection with the Agreement.
	DPO (if applicable) name and contact details:	[Insert details]
	EU Rep (if applicable) name and contact details:	[Insert details]

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1.	Name:	Virtru Corporation
	Contact person's name, position and contact details:	dpa@virtru.com
	Activities relevant to the data transferred under these Clauses:	Processing to carry out the Virtru Services pursuant to the Agreement entered into between Customer and Virtru Corporation.

	Signature and date:	This Annex I shall automatically be deemed executed when the Addendum is executed.
	Role (controller/processor):	Virtru acts as a Processor in relation to all Personal Data Virtru Processes in connection with the Agreement.
	DPO (if applicable) name and contact details:	Not Applicable.
	EU Rep (if applicable) name and contact details:	Not Applicable.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred	Data Subjects include the Customer's employees, individuals that have been provided access by the Customer, and any individual whose Personal Data Customer discloses or makes available to Virtru in connection with the Agreement.
Categories of personal data transferred	The categories of Personal Data transferred are those necessary to operate the service (email address, IP address) and those provided by the Customer, which may be data such as contract information and application-specific data that Customers disclose or make available to Virtru. Other categories of individuals, data, or sensitive information not listed above may be processed by the Customer in emails or files; however, Virtru has no control over the Personal Data processed by the Customer. Information in emails and files processed by the Customer is always encrypted in a manner in which Virtru cannot decrypt the information. The Customer agrees not to process Personal Data in display names for files and email subject lines.
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.	Virtru does not intentionally process special categories of Personal Data; however, the Customer may use Virtru to protect special categories of Personal Data.
The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).	Continuous for all Personal Data.
Nature of the processing	The performance of the Virtru Services.
Purpose(s) of the data transfer and further processing	To perform the Virtru Services.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	As Controller, Customer retains Personal Data for as long as it has a business purpose for it or for the longest time allowable by applicable law. As a Processor, Virtru retains Personal Data it collects or receives from Customer for the duration of the Agreement and consistent with its obligations in this DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	Virtru leverages sub-processors to support all aspects of the platform and provide Virtru Services as described above. See Annex III.

For the purpose of localizing the Standard Contractual Clauses

- Switzerland
  - The parties adopt the GDPR standard for all data transfers.
  - Clause 13 and Annex I(C): The competent authorities under Clause 13, and in Annex I(C), are the Federal Data Protection and Information Commissioner and, concurrently, the EEA member state authority identified above.
  - Clause 17: The parties agree that the governing jurisdiction is the Member State in which the data exporter is established.
  - Clause 18: For Modules 1-3, the parties agree that the forum is the Member State in which the data exporter is established. The parties agree to interpret the Standard Contractual Clauses so that Data Subjects in Switzerland are able to sue for their rights in Switzerland in accordance with Clause 18(c).
  - The parties agree to interpret the Standard Contractual Clauses so that "Data Subjects" includes information about Swiss legal entities until the revised Federal Act on Data Protection becomes operative.
- United Kingdom
  - The parties agree that the Standard Contractual Clauses are deemed amended to the extent necessary that they operate for transfers from the United Kingdom to a Third Country and provide appropriate safeguards for transfers according to Article 46 of the United Kingdom General Data Protection Regulation ("UK GDPR"). Such amendments include changing references to the GDPR to the UK GDPR and changing references to EU Member States to the United Kingdom.
  - Clause 17: The parties agree that the governing jurisdiction is the United Kingdom.
  - Clause 18: For Modules 1-3, the parties agree that the forum is the courts of England and Wales. The parties agree that Data Subjects may bring legal proceedings against either party in the courts of any country in the United Kingdom.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Identify the data exporter's supervisory authority 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 maintains and enforces various policies, standards and processes designed to secure personal data and other data to which Data Importer employees are provided access. Following is a description of some of the core technical and organisational security measures implemented by Data Importer.

Virtru Security Standards

Virtru maintains an information security program that seeks to align with generally accepted standards and is intended to minimize security and privacy risks to the service. Aspects of the information security program include:

> Policies and Procedures – Virtru has adopted and enforces of internal security policies and procedures designed to ensure consistent and uniform implementation of security practices. Policies and procedures include configuration management, incident response, and contingency plans.

Access Controls – Virtru performs background checks of all personnel prior to employment. Virtru provides access to system components only to personnel with a legitimate business need for assigned privileges. Access privileges are revoked when personnel no longer need those privileges to perform assigned job responsibilities. Virtru regularly reviews assigned access permissions to verify continued need.

Awareness – Virtru trains its employees on security practices as well as Virtru policies and procedures to designed to ensure an informed and responsive workforce to security and privacy requirements.

Continuity – Virtru seeks to maintain availability of the service and customer data through replication and backup processes.

Encryption – Virtru seeks to protect personal data it processes by employing encryption of data at rest and data in transit with industry standard encryption mechanisms.

Vulnerability Management – Virtru has implemented processes and industry standard tools for the identification, assessment, and remediation of system vulnerabilities.

Service Provider (Sub-processor) Security – Virtru evaluates prospective and current service providers to confirm that they implement security measures to protect the confidentiality, integrity, and availability of customer data.

Continuous Monitoring – Ongoing evaluation of the security of the environment is performed to identify and respond to risks. Virtru regularly undergoes assessments by independent third-party organizations to ensure the continued effectiveness of the information security program. Virtru evaluates the results of assessments in order to update and improve its information security program in response to security risk and updates in best practices.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

The Controller has authorized the use of the sub-processors disclosed on https://trust.virtru.com/docs/privacy/sub-processors.