DATA PROCESSING ADDENDUM

This Data Processing Addendum (including its Exhibits) ("**Addendum**") forms part of the Terms of Service (the "**Agreement**") between you ("**Company**") and Intuition Machines, Inc. ("**Service Provider**") (collectively the "**Parties**").

1. Subject Matter and Duration.

a) Subject Matter. This Addendum reflects the Parties' commitment to abide by Data Protection Laws concerning the Processing of Company Personal Data in connection with Service Provider's execution of the Agreement. All capitalized terms that are not expressly defined in this Addendum will have the meanings given to them in the Agreement. If and to the extent language in this Addendum or any of its Exhibits conflicts with the Agreement, this Addendum shall control.

b) Duration and Survival. This Addendum will become legally binding upon the effective date of the Agreement. Service Provider will Process Company Personal Data until the relationship terminates as specified in the Agreement. Service Provider's obligations and Company's rights under this Addendum will continue in effect so long as Service Provider Processes Company Personal Data.

2. Definitions.

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

a) "**Company Personal Data**" means Personal Data Processed by Service Provider on behalf of Company.

b) "**Data Protection Laws**" means all applicable data privacy, data protection, and cybersecurity laws, rules and regulations to which the Company Personal Data are subject. "Data Protection Laws" may include, but are not limited to, the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act) ("**CCPA**"); the EU General Data Protection Regulation 2016/679 ("**GDPR**") and its respective national implementing legislations; the Swiss Federal Act on Data Protection; the United Kingdom General Data Protection Regulation; the United Kingdom Data Protection Act 2018; and the Virginia Consumer Data Protection Act (in each case, as amended, adopted, or superseded from time to time).

c) "**Personal Data**" has the meaning assigned to the term "personal data" or "personal information" under applicable Data Protection Laws.

d) "**Process**" or "**Processing**" means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

e) "**Security Incident(s)**" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Company Personal Data attributable to Service Provider.

f) "**Services**" means the services that Service Provider performs under the Agreement.

g) "**Standard Contractual Clauses**" means the Annex to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to

third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

h) "**Subprocessor(s)**" means Service Provider's authorized vendors and third-party service providers that Process Company Personal Data.

3. Processing Terms for Company Personal Data.

a) Documented Instructions. Service Provider shall Process Company Personal Data to provide the Services in accordance with the documented instructions of Company or as specifically authorized by this Addendum, the Agreement, or any applicable Statement of Work. Service Provider will, unless legally prohibited from doing so, inform Company in writing if it reasonably believes that there is a conflict between Company's instructions and applicable law or otherwise seeks to Process Company Personal Data in a manner that is inconsistent with Company's instructions.

b) Authorization to Use Subprocessors. To the extent necessary to fulfill Service Provider's contractual obligations under the Agreement or any Statement of Work, Company hereby authorizes Service Provider to engage Subprocessors. Company acknowledges that Subprocessors may further engage vendors.

c) Service Provider and Subprocessor Compliance. Service Provider agrees to (i) enter into a written agreement with Subprocessors regarding such Subprocessors' Processing of Company Personal Data that imposes on such Subprocessors data protection requirements for Company Personal Data that are consistent with this Addendum; and (ii) remain responsible to Company for Service Provider's Subprocessors' failure to perform their obligations with respect to the Processing of Company Personal Data.

d) Right to Object to Subprocessors. Where required by Data Protection Laws, Service Provider will notify Company via email prior to engaging any new Subprocessors that Process Company Personal Data and allow Company ten (10) days to object. If Company has legitimate objections to the appointment of any new Subprocessor, the Parties will work together in good faith to resolve the grounds for the objection for no less than thirty (30) days.

e) Confidentiality. Any person authorized to Process Company Personal Data must be subject to a duty of confidentiality, contractually agree to maintain the confidentiality of such information, or be under an appropriate statutory obligation of confidentiality.

f) Personal Data Inquiries and Requests. Where required by Data Protection Laws, Service Provider agrees to provide reasonable assistance and comply with reasonable instructions from Company related to any requests from individuals exercising their rights in Company Personal Data granted to them under Data Protection Laws.

g) Data Protection Assessment, Data Protection Impact Assessment, and Prior Consultation. Where required by Data Protection Laws, Service Provider agrees to provide reasonable assistance and information, at Company's expense, to Company where, in Company's judgement, the type of Processing performed by Service Provider requires a data protection assessment, a data protection impact assessment, and/or prior consultation with the relevant data protection authorities.

h) Demonstrable Compliance. Service Provider agrees to provide information reasonably necessary to demonstrate compliance with this Addendum upon Company's reasonable request.

i) California Specific Terms. To the extent that Service Provider's Processing of Company Personal Data is subject to the CCPA, this Section shall also apply. Company discloses or otherwise

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

4. Service Optimization.

a) Where permitted by Data Protection Laws, Service Provider may Process Company Personal Data: (i) for its internal uses to build or improve the quality of its services; (ii) to detect Security Incidents; and (iii) to protect against fraudulent or illegal activity.

b) Aggregation and De-Identification. Service Provider may: (i) compile aggregated and/or de-identified information in connection with providing the Services provided that such information cannot reasonably be used to identify Company or any data subject to whom Company Personal Data relates ("**Aggregated and/or De-Identified Data**"); and (ii) use Aggregated and/or De-Identified Data for its lawful business purposes.

5. Information Security Program.

a) Security Measures. Service Provider shall use commercially reasonable efforts to implement and maintain reasonable administrative, technical, and physical safeguards designed to protect Company Personal Data. Such safeguards shall include those set forth in **Exhibit A**.

6. Security Incidents.

a) Notice. Upon becoming aware of a Security Incident, Service Provider agrees to provide written notice without undue delay and within the time frame required under Data Protection Laws to Company's Designated POC. Where possible, such notice will include all available details required under Data Protection Laws for Company to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

7. Cross-Border Transfers of Company Personal Data.

a) Cross-Border Transfers of Company Personal Data. Company authorizes Service Provider and its Subprocessors to transfer Company Personal Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to the United States.

b) EEA, Swiss, and UK Standard Contractual Clauses (Module Two and Module Three). If Company Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is transferred by Company to Service Provider in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws, the parties agree that the transfer shall be governed by the Standard Contractual Clauses as supplemented by

Exhibit B attached hereto, the terms of which are incorporated herein by reference. Where the Standard Contractual Clauses apply under this Section and Company acts as a controller of Company Personal Data with Service Provider acting as a processor of Company Personal Data, each party shall comply with its obligations under Module Two of the Standard Contractual Clauses. Where the Standard Contractual Clauses apply under this Section and Company acts as a processor of Company Personal Data with Service Provider acting as a (sub)processor of Company Personal Data, each party shall comply with its obligations under Module Three of the Standard Contractual Clauses. Each party's execution of the Agreement shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder. I

c) EEA, Swiss, and UK Standard Contractual Clauses (Module Four). If Company Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is transferred by Service Provider to Company in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws, the parties agree that the transfer shall be governed by Module Four of the Standard Contractual Clauses as supplemented by **Exhibit C** attached hereto, the terms of which are incorporated herein by reference. Each party's execution of the Agreement shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.

8. Audits and Assessments.

a) Company Audit/Assessments. Where Data Protection Laws afford Company an audit or assessment right, Company (or its appointed representative) may carry out an audit or assessment of Service Provider's policies, procedures, and records relevant to the Processing of Company Personal Data. Any audit or assessment must be: (i) conducted during Service Provider's regular business hours; (ii) with forty-five (45) days advance notice to Service Provider; (iii) carried out in a manner that prevents unnecessary disruption to Service Provider's operations; and (iv) subject to reasonable confidentiality procedures. In addition, any audit or assessment shall be limited to once per year, unless an audit or assessment is carried out at the direction of a government authority having proper jurisdiction. Any such audit or assessment shall be subject to Service Provider's security and confidentiality terms and guidelines, and conducted by a mutually agreed upon third party law firm bound by confidentiality rules in order to safeguard Service Provider's obligations to other customers, intellectual property, and trade secrets. In the event that Service Provider and Company cannot agree upon a third-party law firm, the largest law firm on the most recent Am Law 100 list published by American Lawyer (law.com) that agrees to accept the work and has not conducted business with either Service Provider or Company in the preceding 12 months shall be chosen. Company shall be responsible for any costs arising from such audit or assessment.

9. Company Personal Data Deletion.

a) Data Deletion. At the expiry or termination of the Agreement, Service Provider will, at Company's option, delete or return all Company Personal Data (excluding any back-up or archival copies which shall be deleted in accordance with Service Provider's data retention schedule), except where Service Provider is required to retain copies under applicable laws, in which case Service Provider will isolate and protect that Company Personal Data from any further Processing except to the extent required by applicable laws.

10. Processing Details.

a) Subject Matter. The subject matter of the Processing is the Services pursuant to the Agreement.

b) Duration. The Processing will continue until the expiration or termination of the Agreement.

c) Categories of Data Subjects. Data subjects whose Company Personal Data will be Processed pursuant to the Agreement.

d) Nature and Purpose of the Processing. The purpose of the Processing of Company Personal Data by Service Provider is the performance of the Services pursuant to the Agreement.

e) Types of Company Personal Data. Company Personal Data that is Processed pursuant to the Agreement.

11. Contact Information.

a) Company and Service Provider agree to designate a point of contact for urgent privacy and security issues (a "**Designated POC**"). The Designated POC for Company is the representative who registers for the Service. The Designated POC for Service Provider is support@hcaptcha.com.

EXHIBIT A TO THE DATA PROCESSING ADDENDUM

TECHNICAL AND ORGANIZATIONAL MEASURES

This Exhibit A forms part of the Addendum. Capitalized terms not defined in this Exhibit A have the meaning set forth in the Addendum.

Service Provider shall use commercially reasonable efforts to implement and maintain reasonable administrative, technical, and physical safeguards designed to protect Company Personal Data.

Such safeguards shall include controls equivalent to or exceeding the SOC 2 Security Trust Service Principle standard.

EXHIBIT B TO THE DATA PROCESSING ADDENDUM

SUPPLEMENTAL TERMS FOR THE STANDARD CONTRACTUAL CLAUSES (MODULE TWO AND MODULE THREE)

This Exhibit B forms part of the Addendum. Capitalized terms not defined in this Exhibit B have the meaning set forth in the Addendum.

The parties agree that the following terms shall supplement Module Two and Three of the Standard Contractual Clauses:

1. **Supplemental Terms.** The parties agree that: (i) a new Clause 1(e) is added the Standard Contractual Clauses which shall read: "To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties' processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection."; (ii) a new Clause 1(f) is added to the Standard Contractual Clauses which shall read: "To the extent applicable hereunder, these Clauses, as supplemented by Annex III, also apply mutatis mutandis to the Parties' processing of personal data that is subject to UK Data Protection Laws (as defined in Annex III)."; (iii) the optional text in Clause 7 is deleted; (iv) Option 1 in Clause 9 is struck and Option 2 is kept, and data importer must notify data exporter of any new subprocessors in accordance with Section 3(d) of the Addendum; (v) the optional text in Clause 11 is deleted; and (vi) in Clauses 17 and 18, the governing law and the competent courts are those of Ireland (for EEA transfers), Switzerland (for Swiss transfers), or England and Wales (for UK transfers).

2. **Annex I.** Annex I to the Standard Contractual Clauses shall read as follows:

   A. List of Parties

   Data Exporter: Company.
   Address: As set forth in the Notices section of the Agreement.
   Contact person's name, position, and contact details: Company's Designated POC.
   Activities relevant to the data transferred under these Clauses: The Services.
   Role: Controller (Module Two); Processor (Module Three).

   Data Importer: Service Provider.
   Address: As set forth in the Notices section of the Agreement.
   Contact person's name, position, and contact details: Service Provider's Designated POC.
   Activities relevant to the data transferred under these Clauses: The Services.
   Role: Processor (Module Two); Subprocessor (Module Three).

   B. Description of the Transfer:

   Categories of data subjects whose personal data is transferred: The Users of data exporter's or its customer's website, app(s), or other online services.

   Categories of personal data transferred: IP address numbers, device information.

   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: No.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Personal data is transferred in accordance with the standard functionality of the Services on a continuous basis, or as otherwise agreed upon by the parties.

Nature of the processing: The Services.

Purpose(s) of the data transfer and further processing: The Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Data importer will retain personal data in accordance with the Addendum.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

Name of Subprocessor	Subject matter, nature, and duration of processing	Location (Country)	Adequacy Mechanism Supporting Transfer
Cloudflare, San Francisco CA, USA	CDN and edge compute cloud services	Global	SCCs or N/A if Secure Enclave + First-party with Blinding are used by Company.
Microsoft, Redmond WA, USA	Azure cloud services	Global	SCCs or N/A if Secure Enclave + First-party with Blinding are used by Company.
Amazon, Seattle WA, USA	AWS cloud services	Global	SCCs or N/A if Secure Enclave + First-party with Blinding are used by Company.
IBM, Armonk NY, USA	IBM Softlayer cloud services	Global	SCCs or N/A if Secure Enclave + First-party with Blinding are used by Company.

C. Competent Supervisory Authority: The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

D. Additional Data Transfer Impact Assessment Questions:

What countries will personal data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom be stored in or accessed from?

If data exporter utilizes "Secure Enclave" and "First-Party Hosting with IP Blinding" features, no personal data associated with end users is ever transferred outside of the EEA/CH/UK by data importer: personal data is first deidentified by data exporter rather than data importer, in a location of data exporter's choice. If data exporter uses neither feature, personal data associated with end users is in normal (non-automated/abuse/debugging) user scenarios is de-identified at the CDN edge, in a datacenter within the end user's country of access.

Will data importer process any personal data under the Clauses about a non-United States person that is "foreign intelligence information" as defined by 50 U.S.C. § 1801(e)?

Not to data importer's knowledge.

Is data importer subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where personal data is stored or accessed from that would interfere with data importer fulfilling its obligations under the Clauses? For example, FISA Section 702. If yes, please list these laws:

Data importer's HQ is in the United States and is therefore likely subject to United States law. As of the effective date of the Addendum, no court has found data importer to be eligible to receive process issued under the laws contemplated by this question, including FISA Section 702, and no such court action is pending.

Has data importer ever received a request from public authorities for information pursuant to the laws contemplated by the question above? If yes, please explain:

No.

Has data importer ever received a request from public authorities for personal data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain:

No.

E. Data Transfer Impact Assessment Outcome: Taking into account the information and obligations set forth in the Addendum and, as may be the case for a party, such party's independent research, to the parties' knowledge, the personal data originating in the European Economic Area, Switzerland, and/or the United Kingdom that is transferred pursuant to the Clauses to a country that has not been found to provide an adequate level of protection under applicable data protection laws is afforded a level of protection that is essentially equivalent to that guaranteed by applicable data protection laws.

F. Clarifying Terms: The parties agree that: (i) the certification of deletion required by Clause 8.5 and Clause 16(d) of the Clauses will be provided upon data exporter's written request; (ii) the measures data importer is required to take under Clause 8.6(c) of the Clauses will only cover data importer's impacted systems; (iii) the audit described in Clause 8.9 of the Clauses shall be carried out in accordance with Section 8 of the Addendum; (iv) under Module Three, Clause 9(a), data exporter shall be responsible for communicating any changes in subprocessors to the controller; (v) the termination right contemplated by Clause 14(f) and Clause 16(c) of the Clauses will be limited to the termination of the Clauses; (vi) unless otherwise stated by data importer, data exporter will be responsible for communicating with data subjects pursuant to Clause 15.1(a) of the Clauses; (vii) the information required under Clause 15.1(c) of the Clauses will be provided upon data exporter's written request; and (viii) notwithstanding anything to the contrary, data exporter will reimburse data importer for all costs and expenses incurred by data importer in connection with the performance of data importer's obligations under Clause 15.1(b) and Clause 15.2 of the Clauses without regard for any limitation of liability set forth in the Agreement.

3. **Annex II.** Annex II of the Standard Contractual Clauses shall read as follows:

   Data importer shall implement and maintain technical and organisational measures designed to protect personal data in accordance with **Exhibit A**.

   Pursuant to Clause 10(b), data importer will provide data exporter assistance with data subject requests in accordance with the Addendum.

4. **Annex III.** A new Annex III shall be added to the Standard Contractual Clauses and shall read as follows:

The UK Information Commissioner's Office International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("**UK Addendum**") is incorporated herein by reference.

Table 1: The start date in Table 1 is the effective date of the Addendum. All other information required by Table 1 is set forth in Annex I, Section A of the Clauses.

Table 2: The UK Addendum forms part of the version of the Approved EU SCCs which this UK Addendum is appended to including the Appendix Information, effective as of the effective date of the Addendum.

Table 3: The information required by Table 3 is set forth in Annex I and II to the Clauses.

Table 4: The parties agree that Importer may end the UK Addendum as set out in Section 19.

EXHIBIT C TO THE DATA PROCESSING ADDENDUM

SUPPLEMENTAL TERMS FOR THE STANDARD CONTRACTUAL CLAUSES (MODULE FOUR)

This Exhibit C forms part of the Addendum. Capitalized terms not defined in this Exhibit C have the meaning set forth in the Addendum.

Throughout the term of the Agreement, Company will promptly notify Service Provider's Designated POC within ten (10) business days if there are material changes to the responses set forth in Section 2(C) – 2(D) of this Exhibit C following the effective date of the Agreement and work with Service Provider to update Company's responses set forth in this Exhibit C.

The parties agree that the following terms shall supplement the Standard Contractual Clauses:

1. **Supplemental Terms.** The parties agree that: (i) a new Clause 1(e) is added the Standard Contractual Clauses which shall read: "To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties' processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection."; (ii) a new Clause 1(f) is added to the Standard Contractual Clauses which shall read: "To the extent applicable hereunder, these Clauses, as supplemented by Annex II, also apply mutatis mutandis to the Parties' processing of personal data that is subject to UK Data Protection Laws (as defined in Annex II)."; (iii) the optional text in Clause 7 is deleted; (iv) the optional text in Clause 11 is deleted; and (vi) in Clauses 17 and 18, the governing law and the competent courts are those of Ireland (for EEA transfers), Switzerland (for Swiss transfers), or England and Wales (for UK transfers).

2. **Annex I.** Annex I to the Standard Contractual Clauses shall read as follows:

   A. List of Parties

   Data Exporter: Service Provider.
   Address: As set forth in the Notices section of the Agreement.
   Contact person's name, position, and contact details: Service Provider's Designated POC.
   Activities relevant to the data transferred under these Clauses: The Services.
   Role: Processor.

   Data Importer: Company.
   Address: As set forth in the Notices section of the Agreement.
   Contact person's name, position, and contact details: Company's Designated POC.
   Activities relevant to the data transferred under these Clauses: The Services.
   Role: Controller.

   B. Description of the Transfer:

   Categories of data subjects whose personal data is transferred: The categories of data subjects whose personal data will be provided under the Clauses which may include, but are not limited to, those data subjects listed in Exhibit B.

   Categories of personal data transferred: The categories of personal data that will be provided under the Clauses which may include, but are not limited to, the categories of personal data listed in Exhibit B.

   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: No.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Personal data is transferred in accordance with the standard functionality of the Services, or as otherwise agreed upon by the parties.

Nature of the processing: The Services.

Purpose(s) of the data transfer and further processing: The operation of data importer's business.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Data importer will retain personal data in accordance with the applicable data importer privacy notice or policy that governs such personal data.

C. Additional Data Transfer Impact Assessment Questions:

What countries will Company Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom be stored in or accessed from by Company? If this varies by region, please specify each country for each region.

Those countries where data importer conducts its business activities which may include, but are not limited to, the United States.

Will data importer process any personal data under the Clauses about a non-United States person that is "foreign intelligence information" as defined by 50 U.S.C. § 1801(e)?

Not to data importer's knowledge.

Is data importer subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where personal data is stored or accessed from that would interfere with data importer fulfilling its obligations under the Clauses? For example, FISA Section 702. If yes, please list these laws:

As of the effective date of the Addendum, no court has found data importer to be eligible to receive process issued under the laws contemplated by this question, including FISA Section 702, and no such court action is pending.

Has data importer ever received a request from public authorities for information pursuant to the laws contemplated by the question above? If yes, please explain:

No.

Has data importer ever received a request from public authorities for personal data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain:

No.

D. Data Transfer Impact Assessment Outcome: Taking into account the information and obligations set forth in the Addendum and, as may be the case for a party, such party's independent research, to the parties' knowledge, the personal data originating in the European Economic Area, Switzerland, and/or the United Kingdom that is transferred pursuant to the Clauses to a country that has not been found to provide an adequate level of protection under applicable data protection laws is afforded a level of protection that is essentially equivalent to that guaranteed by applicable data protection laws.

E. Clarifying Terms: The parties agree that: (i) the information required by Clause 8.1(d) of the Clauses will be provided upon data importer's written request; and (ii) the audit described in Clause 8.3(b) of the Clauses shall be carried out in accordance with Section 8 of the Addendum.

3. **Annex II.** A new Annex II shall be added to the Standard Contractual Clauses and shall read as follows:

The UK Information Commissioner's Office International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("**UK Addendum**") is incorporated herein by reference.

Table 1: The start date in Table 1 is the effective date of the Addendum. All other information required by Table 1 is set forth in Annex I, Section A of the Clauses.

Table 2: The UK Addendum forms part of the version of the Approved EU SCCs which this UK Addendum is appended to including the Appendix Information, effective as of the effective date of the Addendum.

Table 3: The information required by Table 3 is set forth in Annex I to the Clauses.

Table 4: The parties agree that Exporter may end the UK Addendum as set out in Section 19.