InfluxData Inc.
Global Customer Data Processing Addendum

This Global Data Processing Addendum ("**DPA**") applies where InfluxData Inc. on behalf of itself and its affiliates, ("**InfluxData**") and the Customer indicated below ("**Customer**") have entered into one or more Agreements which reference this DPA and pursuant to which InfluxData may process Personal Data on behalf of Customer in order to provide the Services outlined under the Agreement. Any capitalized terms not defined in this DPA shall have the meaning set forth in the Agreement.

Signatures of assent of InfluxData and Customer to this DPA will be deemed signature to, and acceptance and agreement of, this DPA and the SCCs attached hereto.

For the avoidance of doubt, this DPA shall not apply and is not legally valid to any Agreements that explicitly incorporate a separate data processing agreement, provided such separate data processing agreement has been signed by an authorized InfluxData signatory.

INFLUXDATA, INC.	**Customer:**
Address: 548 Market St, PMB 77953, San Francisco, CA 94104	**Address**:
Privacy contact (including for notices): **Name:** Peter Albert **Title:** Chief Information Security Officer **Contact details:** privacy@influxdata.com	**Privacy contact (including for notices):** **Name:** **Title:** **Contact details:**
Signature:	**Signature:**
Name:	**Name:**
Title:	**Title:**
Date Signed:	**Date Signed:**

1. Definitions

1.1 "Agreement" means, collectively, the written or electronic services agreement and the Order Form or any other ordering documents between Customer and InfluxData for the provision of the Services to Customer which explicitly reference this DPA.

1.2 "Applicable Privacy Laws" means any privacy laws or regulations to the extent applicable to the processing of Personal Data under the Agreement, including any binding laws or regulations ratifying, implementing, adopting, supplementing or replacing the foregoing; in each case, to the extent in force, and as such are updated, amended or replaced from time to time.

1.3 "Authorized Personnel" means an employee or agent of InfluxData who is authorized to process Personal Data under the authority of InfluxData.

1.4 "Data Subject Request" means a request from a data subject to exercise their data subject rights with respect to the Personal Data, as granted by Applicable Privacy Laws.

1.5 "Instructions" means Customer's written instructions to InfluxData directing InfluxData to process the Personal Data as provided to Customer under the Agreement, this DPA, or through Customer's use of the features and functionality of the Services or as otherwise mutually agreed by both parties in writing.

1.6 "Personal Data" means any data which is (i) defined as "Personal Data" "Personal Information" "Personally Identifiable Information" or any substantially similar term under Applicable Privacy Laws and (ii) processed on behalf of InfluxData by Vendor (including Authorized Personnel, Sub-Processors, or affiliates) in connection with the Agreement.

1.7 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data in InfluxData's possession or under its control (including when transmitted or stored by InfluxData).

1.8 "Sell" or "selling" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Data to another business or a third party for monetary or other valuable consideration.

1.9 "Services" means the services as described in the Agreement.

1.10 "Share" or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to a third party for cross-context behavioral advertising (as that term is defined in the California Consumer Privacy Act), whether or not for monetary or other valuable consideration.

1.11 "Standard Contractual Clauses" or ("SCCs" or "Clauses") means the standard contractual clauses approved by the European Commission for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

1.12 "Subprocessor" means any person or entity appointed by InfluxData in connection with the processing of Personal Data in connection with the Agreement.

In this DPA, the following terms (and any substantially similar terms as defined under Applicable Privacy Laws) shall have the meanings and otherwise be interpreted in accordance with Applicable Privacy Law: **Business**, **Data Controller, Data Processor, Data Subject**, **Service Provider, Supervisory Authority, process(ing)** and **transfer.**

2. Processing of Data

2.1 The parties acknowledge and agree that with respect to processing of Personal Data, InfluxData is a Data Processor and a Service Provider and Customer is a Data Controller and Business, except that where Customer is a Data Processor in which case InfluxData is a sub-processor of Customer. If Customer is a Data Processor of Personal Data, Customer represents and warrants that Customer's instructions and processing of Personal Data, including its appointment of InfluxData as a sub-processor, have been authorized by the respective Data Controller. For the avoidance of doubt, this DPA does not apply to Personal Data for which InfluxData is an independent controller. InfluxData will not: (i) Sell or Share Customer Personal Data; (ii) use, retain, or disclose Customer Personal Data outside of its direct business relationship with Customer; (iii) use, retain, or disclose Customer Personal Data for any other purpose (including any other commercial purpose) other than as set forth in the Agreement and DPA, except as required by law; or (iv) combine Customer Personal Data with Personal Data that it (a) receives from or on behalf of third parties, or (b) collects from InfluxData's own interactions with data subjects unrelated to the Services. InfluxData shall have rights to process Customer Personal Data:

2.1.1 as necessary or appropriate: (a) for its rights and obligations under the Agreement and this DPA; (b) to operate, manage, test, maintain and enhance the Services including as part of its business operations; (c) to deidentify or aggregate Customer Personal Data in a manner that prevents individual identification of the Customer, or data subjects; and (d) protect the Services from a threat to the Services, Customer or other customers, Customer Personal Data, and InfluxData's systems;

2.1.2 if disclosure is required by Applicable Privacy Laws or other applicable laws, or by court order of a court or authorized governmental agency, provided that prior notice first be given to the Customer unless such notice is prohibited by law or court order; or

2.1.3 as otherwise expressly authorized by the Customer.

2.2 This DPA applies where and solely to the extent that InfluxData processes Personal Data on behalf of Customer for the purpose of providing the Services to the Customer pursuant to the Agreement (the "**Business Purpose**"). The subject matter, nature, purpose, and duration of processing, as well as the types of Personal Data collected and categories of Data Subjects, are as described in Exhibit A.

2.3 InfluxData shall process Personal Data only for the purposes set forth in the Agreement and in accordance with this DPA, the Instructions, and its obligations under Applicable Privacy Laws. InfluxData shall promptly notify Customer if an Instruction, in InfluxData's opinion, infringes Applicable Privacy Laws. InfluxData will also notify Customer if in its opinion it cannot meet its obligations under Applicable Privacy Laws. Customer can take reasonable and appropriate steps to stop unauthorized processing of Company Personal Data.

2.4 Customer shall, in its use of the Services, at all times process Personal Data, and provide the Instructions for the processing of Personal Data, in compliance with Applicable Privacy Laws. Customer represents and warrants that Customer has obtained or will obtain, all necessary consents, licenses and approvals for the processing of Personal Data under this DPA and, where applicable, has a valid legal basis under Applicable Privacy Laws for the processing of Personal Data under this DPA. Customer further represents and warrants that Customer (i) will comply with all Applicable Privacy Laws in its performance arising out of this DPA; and (ii) has reviewed InfluxData's security practices and acknowledges that such practices are appropriately designed to ensure a level of security appropriate to the risk of processing hereunder.

2.5 Following completion of the Services, InfluxData shall return or delete the Personal Data as set forth under the Agreement or applicable service documentation, or provide Customer the ability to delete such Personal Data directly through the tools or functionality made available by the Service. The foregoing obligations shall not apply (a) where deletion is not permitted under applicable law (including Applicable Privacy Laws) or the order of a governmental or regulatory body; (b) where InfluxData retains such Personal Data for internal record keeping and compliance with any legal obligations; or (c) where InfluxData's then-current data retention or similar back-up system stores Personal Data, provided such data will remain protected in accordance with the measures described in the Agreement and this DPA.

3. Authorized Personnel

3.1 InfluxData shall ensure that all Authorized Personnel are made aware of the confidential nature of Personal Data and have executed confidentiality agreements or are otherwise subject to binding duties of confidentiality that prohibit them from disclosing or otherwise processing, any Personal Data except in accordance with the Instructions and their obligations in connection with the Services.

3.2 InfluxData shall take commercially reasonable steps to ensure the reliability and appropriate training of any Authorized Personnel.

4. InfluxData Subprocessors

4.1 Customer hereby provides InfluxData with general written authorization to engage Subprocessors to access and process Personal Data in connection with the Services in accordance with this Section 4.

4.2 A list of InfluxData's current Subprocessors (the "**Subprocessor List**") is available at www.influxdata.com/legal (such URL may be updated by InfluxData from time to time upon notice to Customer). These Subprocessors will be deemed authorized by Customer to process Personal Data in connection with this DPA. At least thirty (30) days before enabling any new Subprocessor to access or participate in the processing of Personal Data, InfluxData will add such Subprocessor to the Subprocessor List and notify Customer of that update by sending an email notification to the email address provided by Customer in the signature block above. Customer may object to such an engagement on reasonable data protection grounds by providing notice to InfluxData within thirty (30) days of receipt of the aforementioned notice from InfluxData.

4.2.1 If Customer objects to an engagement in accordance with Section 4.2, InfluxData shall provide Customer with a written description of commercially reasonable alternative(s), if any, to such engagement. If InfluxData, in its sole discretion, cannot reasonably provide any such alternative(s), or if Customer does not agree to any such alternative(s) if provided, Customer may terminate the impacted Services. Alternatively, Customer's continued use of the Service following Customer's refusal of the proffered alternative will constitute Customer's consent for such a change to the Subprocessor List. Termination shall not relieve Customer of any fees owed to InfluxData under the Agreement.

4.2.2 If Customer does not object to the engagement of a third party in accordance with Section 4.2, that third party will be deemed an authorized Subprocessor for the purposes of this DPA.

4.3 InfluxData will have written contractual obligations with each Subprocessor regarding the processing of Personal Data that are substantially similar to those which InfluxData is subject under this DPA.

4.4 InfluxData shall be liable to Customer for any breach of this DPA caused by the acts or omissions of its Subprocessors.

4.5 If Customer and InfluxData have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the above authorizations will constitute Customer's prior written consent to the subcontracting by InfluxData of the processing of Personal Data if such consent is required under the Standard Contractual Clauses.

5. Security of Personal Data

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, InfluxData shall maintain appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk presented by the processing of the Personal Data. Such technical and organizational measures shall include measures equal to or exceeding the measures set forth in Exhibit B of this DPA.

6. Transfers of Personal Data

6.1 Customer acknowledges and agrees that InfluxData and its Subprocessors may provide the Services from any state, province, country or other jurisdiction. As such, Customer instructs InfluxData and its Subprocessors to transfer and process Personal Data anywhere in the world where InfluxData or its Subprocessors offer data processing operations (current locations of data processing operations are set forth at www.influxdata.com/legal). InfluxData will at all times provide an adequate level of protection for the Personal Data processed, in accordance with the requirements of Applicable Privacy Law.

6.2 With regard to countries, regions or territories with Applicable Privacy Laws requiring a mechanism for valid export of Personal Data (such countries, regions, or territories, "**Limited Transfer Region(s)**" and such data "**Limited Transfer Data**"), neither InfluxData nor its Sub-processors may receive and process such Limited Transfer Data outside of such Limited Transfer Regions unless it or its Sub-processors take measures to adequately protect such data consistent with Applicable Privacy Laws.

Such measures may include to the extent available and applicable under such laws:

6.2.1 Processing in a country, a territory, or one or more specified sectors that are considered under Applicable Privacy Laws as providing an adequate level of data protection;

6.2.2 The parties' agreement to enter into and comply with the Standard Contractual Clauses in Exhibit C and any successors or amendments to such clauses or such other applicable contractual terms adopted and approved under Applicable Privacy Laws;

6.2.3 Processing in compliance with Binding Corporate Rules in accordance with Applicable Privacy Laws; or

6.2.4 Implementing any other data transfer mechanisms or certifications approved under Applicable Privacy Laws, including, as applicable, any approved successor or replacement to the EU–US Privacy Shield framework and/or the Swiss–US Privacy Shield framework.

6.3 The Parties acknowledge and agree that they have, taking into account, without limitation, the Personal Data and third countries in scope, the relevant security measures under this DPA and the relevant parties participating in the processing of such Personal Data, conducted an assessment of the appropriateness of the relevant transfer mechanism adopted hereunder and have determined that such transfer mechanism is appropriately designed to ensure Personal Data transferred in accordance with this DPA a level of protection in the destination country that is essentially equivalent to that guaranteed under the Applicable Privacy Laws

6.4 To the extent that any substitute or additional appropriate safeguards or mechanisms under any Applicable Privacy Laws of Limited Transfer Regions are required to transfer data from a Limited Transfer Region, as applicable, to any third country, the parties agree to implement the same as soon as practicable and document such requirements for implementation in an attachment to this DPA governing the parties' processing of Limited Transfer Data.

7. Cooperation; Audit and Records Requests

7.1 InfluxData shall, to the extent permitted by law, promptly notify Customer following the receipt and verification of a Data Subject Request or shall otherwise advise the Data Subject to submit their Data Subject Request to Customer directly. In either case, Customer will be responsible for responding to such request.

7.2 At the request of Customer and taking into account the nature of the processing applicable to any Data Subject Request, InfluxData shall apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance *provided that* (i) Customer is itself unable to respond or fulfill the request without InfluxData's assistance and (ii) InfluxData is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by InfluxData.

7.3 InfluxData shall, taking into account the nature of the processing and the information available to InfluxData provide Customer with reasonable cooperation and assistance for Customer to: (i) understand how InfluxData processes Customer Personal Data in line with the DPA and Applicable Privacy Laws it is subject to; (ii) comply with its obligations under Applicable Privacy Law (and to demonstrate the same), (iii) conduct a data protection impact assessment and, (iv) respond to any inquiry or consultation with any Supervisory Authority. The obligations hereunder shall only apply where required of InfluxData by Applicable Privacy Law and provided that Customer does not otherwise have access to the relevant information or functionality being requested. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by InfluxData.

7.4 Upon Customer's request and no more than once per calendar year, InfluxData shall make available for Customer's review copies of certifications or reports demonstrating InfluxData's compliance with Applicable Privacy Laws as they relate to the processing of Customer's Personal Data.

8. Personal Data Breach

8.1 After becoming aware of a Personal Data Breach, InfluxData shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as InfluxData, in its sole discretion, deems necessary and reasonable to remediate such Personal Data Breach (to the extent that remediation is within InfluxData's reasonable control).

8.2 InfluxData shall, taking into account the nature of the processing and the information reasonably available to InfluxData: (a) provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under Applicable Privacy Laws with respect to notifying relevant regulators and/or Data Subjects affected by such Personal Data Breach; and (b) provide Customer with information in InfluxData's reasonable control concerning the details of the Personal Data Breach including, as applicable, the nature of the Personal Data Breach, the categories and approximate numbers of Data Subjects and Personal Data records concerned, and the likely consequences of the Personal Data Breach.

8.3 The obligations described in this Section 8 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. In no event will InfluxData's cooperation or obligation to report or respond to a Personal Data Breach under this Section be construed as an acknowledgement by InfluxData of any fault or liability with respect to the Personal Data Breach.

9. Miscellaneous

9.1 The liability of InfluxData and its respective employees, directors, officers, affiliates, successors, and assigns (the "**InfluxData Parties**"), arising out of or related to this DPA, whether in contract, tort, or other theory of liability, shall be subject to the "Limitation of Liability" and "Exclusions of Liability" sections (or their equivalent sections) of the Agreement, and any reference in such section to the liability of InfluxData or the InfluxData Parties means the aggregate liability of the InfluxData Parties under the Agreement and this DPA together.

9.2 This DPA is without prejudice to the rights and obligations of the parties under the Agreement which will continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA will prevail insofar as the subject matter concerns the processing of Personal Data. In the event of any conflict between the terms of this DPA and the Standard Contractual Clauses then, only insofar as the Standard Contractual Clauses apply, the Standard Contractual Clauses will prevail.

9.3 Customer and InfluxData each agree that the dispute resolution provisions of the Agreement (including governing law and venue) apply to this DPA.

EXHIBIT A
Details of Processing

Data exporter:
The data exporter is: Customer

Data importer:
The data importer is: InfluxData Inc. and its affiliates

Data subjects:
The personal data transferred concern the following categories of data subjects: Data exporter's, its affiliates, and its and their service providers', employees, consultants, agents and representatives authorized by data exporter to use the Services.

Categories of data:
Data exporter may submit Personal Data to data importer, and which may include, but is not limited to the following categories of personal data: (a) First and last name; (b) Title; (c) Position; (d) Employer; (e) Contact information (company, email, phone, physical business address); (f) IP address; (g) any other Personal Data data exporter chooses to provide to the Services in accordance with the Agreement.

Special categories of data (if appropriate):
N/A

Nature and business purpose of processing operations:
The objective of the processing of Personal Data by data importer is the performance of the Services related to the Agreement with the data exporter. These Services include making the data importer platform, tools, and services available to data exporter for the data exporter built or selected applications and use cases, which when determined by data exporter, may involve processing of Personal Data in connection with the data exporter built or selected applications. This processing may include collection, storage, retrieval, consultation, use, erasure or destruction, disclosure by transmission, dissemination or otherwise making available data exporter's Personal Data as necessary to provide the Services to data importer in accordance with the data exporter's instructions and Applicable Privacy Law.

Duration of processing:
InfluxData will Process Customer Personal Data while the Agreement and DPA remain in effect and InfluxData continues to process Customer Personal Data pursuant to the Agreement and DPA.

EXHIBIT B
Technical and Organizational Security Measures

InfluxData will maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Customer Personal Data, equal to or better than those described in the Customer Data Security Exhibit published at https://influxdata.com/legal. InfluxData regularly monitors compliance with these safeguards.

EXHIBIT C
Standard Contractual Clauses

The parties agree that Limited Transfer Data transferred between and among the parties shall be subject to the standard contractual clauses to the extent applicable. Without limitation: (i) transfers of Limited Transfer Data from the European Economic Area ("EEA") or Switzerland (or Limited Transfer Data subject to Applicable Privacy Laws in the EEA or Switzerland) to jurisdictions that have not been deemed to provide an adequate level of protection for personal data by the EU are subject to the Standard Contractual Clauses in this Exhibit C; (ii) transfers of Limited Transfer Data from the United Kingdom ("UK") (or Limited Transfer Data subject to Applicable Privacy Laws in the UK) to jurisdictions that have not been deemed to provide an adequate level of protection for personal data by the UK are subject to the Standard Contractual Clauses in this Exhibit C as supplemented by the UK Transfer Addendum in this Exhibit C.

(A) The parties acknowledge the importance of the protection of Personal Data and the legal restrictions on international transfers of Personal Data.

(B) Accordingly, the parties agree to abide by the GDPR, UK GDPR and Data Protection Act 2018, and Swiss Federal Data Protection Act, and other Applicable Privacy Laws of Limited Transfer Regions recognizing the Standard Contractual Clauses or similar principles, as applicable, and enter into these standard contractual clauses to ensure that Personal Data transfers outside any Limited Transfer Regions to any third country other than a country, region, or territory that the relevant data authority has determined to offer an adequate level of data protection are lawful and subject to adequate data protections. To the extent Personal Data is subject to Article 3(2) of the GDPR, this Exhibit C shall not apply.

1. CLARIFICATION OF DEFINITIONS & TERMS

(A) The terms "data controller" or "controller," "data exporter," "data importer," "data processor" and "Personal Data" shall have the meaning under the GDPR, UK GDPR and Data Protection Act 2018, Swiss Federal Data Protection Act, or Applicable Privacy Laws of Limited Transfer Regions as applicable.

(B) For Limited Transfer Regions outside the EU, references to the General Data Protection Regulation will be replaced by Applicable Privacy Laws of the respective Limited Transfer Regions. If Switzerland is the Limited Transfer Region: references to "Regulation (EU) 2016/679" and any articles therefrom shall be interpreted to include references to the Swiss DPA; and references to "EU", "Union" and "Member State" shall be interpreted to include references to "Switzerland".

(C) Section 1 Clause 1 (a) of the Standard Contractual Clauses (Definition of Data Importer): The "data importer" means InfluxData.

(D) Section 1 Clause 1 (a) of the Standard Contractual Clauses (Definition of Data Exporter): The "data exporter" means Customer.

(E) With respect to objections to subprocessors under Section 1 Clause 9, the parties will work together to find a mutually acceptable resolution to such objection, and if unsuccessful, Customer's sole remedy is termination of the relevant Services under the terms of the Agreement

2. APPLICABLE MODULES

With respect to Processing of Customer Personal Data,

(A) When Customer is a Data Exporter and Controller, and InfluxData is a Data Importer and Processor - Module 2 shall apply.

(B) When Customer is a Data Exporter and Processor, and InfluxData is a Data Importer and Sub-Processor - Module 3 shall apply.

3. AMENDMENTS OR UPDATES

The parties agree that to the extent that any additional appropriate safeguards under Applicable Privacy Laws of Limited Transfer Regions recognizing the Standard Contractual Clauses or similar principles are required to export data to any third country, or to the extent that the Standard Contractual Clauses are substituted or replaced or not recognised under any such law, the parties agree to either promptly implement the same or agree to use another acceptable method for transfer of such data and promptly amend this Exhibit C as necessary to comply with such requirements.

4. CONFLICTS

If the terms of the Agreement or the DPA conflict with the Standard Contractual Clauses, the terms of the Standard Contractual Clauses will prevail.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 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) 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')

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

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 – *Module Two*: Clause 8.1(b), 8.9(a), (c), (d) and (e); *Module Three*: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

iii.Clause 9 – *Module Two*: Clause 9(a), (c), (d) and (e); *Module Three*: Clause 9(a), (c), (d) and (e);

iv.Clause 12 – *Modules Two and Three*: Clause 12(a), (d) and (f);

v.Clause 13;

vi.Clause 15.1(c), (d) and (e);

vii.Clause 16(e);

viii.Clause 18 – *Modules Two and Three*: 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 - Docking clause [Optional]

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: Transfer 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 (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 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.

MODULE THREE: Transfer processor to processor

8.1 Instructions

a. The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

b. The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

c. The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

d. The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by 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 of Regulation (EU) 2016/679;

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 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 or the controller 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 controller.

c. The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

d. The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

e. Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

f. 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.

g. 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. 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 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.

MODULE THREE: Transfer processor to processor

a. The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller 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 controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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

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.

MODULE THREE: Transfer processor to processor

a. The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

b. The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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:

1. 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;
2. 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. ***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

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 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). [***For Module Three***: The data exporter shall forward the notification to the controller.]

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 [***for Module Three***:, if appropriate in consultation with the controller]. 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 [***for Module Three***: the controller or] 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.

[***For Module Three***: The data exporter shall forward the notification to the controller.]

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.). [***For Module Three***: The data exporter shall forward the information to the controller.]

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. [***For Module Three***: The data exporter shall make the assessment available to the controller.]

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 [***for Module Three***: and the controller] 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.

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 the EU Member State 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 third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

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 Ireland.

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
DETAILS OF PROCESSING

A. LIST OF PARTIES

Data exporter(s):

Name: Customer

Address: As set forth in signature block of the DPA

Contact person's name, position and contact details: As set forth in signature block of the DPA

Activities relevant to the data transferred under these Clauses: Receipt of the Services under the Agreement

Signature and date: Signature of assent of Customer to the DPA will be deemed signature to the SCCs.

Role (controller/processor): Controller (or processor acting on behalf of a controller)

Data importer(s):

Name: InfluxData Inc.

Address: As set forth in signature block of the DPA

Contact person's name, position and contact details: As set forth in signature block of the DPA

Activities relevant to the data transferred under these Clauses: Provision of the Services under the Agreement

Signature and date: Signature of assent of InfluxData to the DPA will be deemed signature to the SCCs.

Role (controller/processor): Processor (or sub-processor where InfluxData is acting as a processor) of Customer

B. DESCRIPTION OF TRANSFER

Intentionally omitted - refer to Exhibit A

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority shall be the supervisory authority of the Member State chosen as the governing law in accordance with Clause 17 of the Standard Contractual Clauses.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Intentionally omitted - refer to Exhibit B

UK TRANSFER ADDENDUM TO STANDARD CONTRACTUAL CLAUSES

Information Commissioner's Office

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Customer, as set forth in signature block of the DPA. Trading name (if different):	Full legal name: InfluxData, Inc. Trading name (if different):

	Main address (if a company registered address): As set forth in the signature block of the DPA. Official registration number (if any) (company number or similar identifier):	Main address (if a company registered address): As set forth in the signature block of the DPA. Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): As set forth in the signature block of the DPA. Job Title: As set forth in the signature block of the DPA. Contact details including email: As set forth in the signature block of the DPA.	Full Name (optional): As set forth in the signature block of the DPA. Job Title: As set forth in the signature block of the DPA. Contact details including email: As set forth in the signature block of the DPA.
Signature (if required for the purposes of Section 2)	Signature of assent of Customer to the DPA will be deemed signature to this UK Transfer Addendum.	Signature of assent of InfluxData, Inc. to the DPA will be deemed signature to this UK Transfer Addendum.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Effective Date of the DPA. Reference (if any): Standard Contractual Clauses as contained in this Exhibit C to the DPA. Other identifier (if any):

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	N/A. As described in the version of Standard Contractual Clauses contained in this Exhibit C to the DPA.					
2						
3						
4						

Table 3: Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: InfluxData Inc. and Customer as provided in Annex I to the SCCs in this Exhibit C to the DPA.
Annex 1B: Description of Transfer: Refer to Exhibit A of the DPA.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Refer to Exhibit B of the DPA.
Annex III: List of Sub processors (Modules 2 and 3 only): Refer to Section 4.2 of the DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**: Exporter and/or Importer

Part 2: Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, 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 **Error! Reference source not found.** of those Mandatory Clauses.