DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the Service Agreement or other written or electronic agreement between IIJ and Customer for the purchase of online services (including associated IIJ offline or mobile components) from IIJ (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "**Services**") (the "**Agreement**") to reflect the parties' agreement with regard to the Processing of Personal Data.

By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent IIJ processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, IIJ may process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

HOW THIS DPA APPLIES:

(i) The Customer signing this DPA is a party to a Service Agreement between the Customer and IIJ. This DPA is an addendum to and forms part of the Service Agreement.

(ii) This DPA shall not replace any comparable or additional rights relating to Processing of Customer Data contained in the Service Agreement (including any existing data processing addendum to the Agreement).

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1, 2, 3 and 4 (including Appendices attached thereto). For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules and Appendices.

2. By signing the application form to enter into the Service Agreement, the Customer and IIJ shall be deemed to constitute signature and acceptance of the Schedules to the DPA, including their Appendices, to the extent applicable and in order of precedence as specified in Section 11 of the DPA. Where Customer wishes to separately execute Schedule 4 of the DPA, Customer should also complete the information as the data exporter on Page 27 and complete the information in the signature box and sign on Pages 32, 34, 35 and 36.

3. The parties may execute this DPA in counterparts, each of which is deemed an original, but all of which together constitute one and the same agreement. This DPA may be delivered by facsimile transmission or by email exchange of PDF file, and facsimile copies or PDF files of executed signature pages shall be binding as originals.

Once executed by both Customer and IIJ, this DPA will become legally binding.

1. DATA PROCESSING TERMS

1.1 INTERPRETATION

The definitions used in this DPA shall have the meanings set forth in this DPA, unless the context requires otherwise. Capitalised terms used, but not defined, in this DPA will have the meanings given to them in the Service Agreement. Except as modified or supplemented below, the definitions of the Service Agreement, as well as the other terms and conditions of the Service Agreement, shall remain in full force and effect.

1.2 DEFINITIONS

For the purpose of interpreting this DPA, the following terms shall have the meanings set out below:

a. **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

b. **"Authorized Affiliate"** means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and IIJ, but has not signed its own order form ("**Order Form**") with IIJ and is not a "Customer" as defined under the Agreement.

c. **"Controller"** means the entity which determines the purposes and means of the Processing of Personal Data.

d. **"Customer Data"** means what is defined in the Agreement as "Customer Data" or "Your Data."

e. **"Data Protection Laws and Regulations"** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and/or the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

f. **"Data Subject"** means the identified or identifiable person to whom Personal Data relates.

g. **"GDPR"** means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation), including as implemented or adopted under the laws of the United Kingdom.

h. **"Personal Data"** means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected in a manner similar to that of personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

i. **"Processing"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.

j. **"Processor"** means the entity which Processes Personal Data on behalf of the Controller.

k. **"IIJ"** means the IIJ entity which is a party to this DPA, as specified in the section "HOW THIS DPA APPLIES" above.

l. **"IIJ Group"** means IIJ and its Affiliates engaged in the Processing of Personal Data.

m. **"IIJ Processor BCR"** means IIJ's Processor binding corporate rules for the Processing of Personal Data, the updated versions of which are available by scrolling down to the Binding Corporate Rules section on IIJ's webpage "IIJ Group Global Privacy Policy", accessible at https://www.iij.ad.jp/en/privacy/global/ , which govern transfers of Personal Data (i) among IIJ Group members who act as Processor or Sub-processor, or (ii) from a Customer established in the European Economic Area member states or Switzerland whose processing activities for the relevant data are governed by the GDPR and/or implementing national legislation to an IIJ Group member who acts as a Processor, or (iii) from non-European Economic Area member states for which Customer has contractually specified that the GDPR and implementing national legislation shall apply, to an IIJ Group member who acts as a Processor, or (iv) from an IIJ Group member who acts as a Processor to a non-IIJ Group Sub-processor located outside the European Economic Area.

n. **"Standard Contractual Clauses 2021"** or **"SCC 2021"** means the agreement executed by and between Customer and IIJ and attached hereto as Schedule 3 pursuant 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.

o. **"Standard Contractual Clauses 2010"** or **"SCC 2010"** means the agreement executed by and between Customer and IIJ and attached hereto as Schedule 4 pursuant to the European Commission's decision (C(2010)593) of 5

February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, and to paragraph 7(2) of Schedule 21 to the Data Protection Act 2018 of the United Kingdom.

p. **"Sub-processor"** means any Processor engaged by IIJ or a member of the IIJ Group to process Personal Data in connection with the Agreement.

q. "**Supervisory Authority**" means an independent public authority which is established by an EU Member State or the United Kingdom pursuant to the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller (or processor as the case may be), IIJ is the Processor (or sub-processor as the case may be) as further specified in the Details of the Processing (Schedule 1) and that IIJ or members of the IIJ Group will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2 Customer shall, in its use of the Services, process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3 IIJ shall treat Personal Data as Confidential Information and shall only process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.4 The subject-matter of Processing of Personal Data by IIJ is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 IIJ shall, to the extent legally permitted, promptly notify Customer if IIJ receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure (right to be forgotten), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("**Data Subject Request**").

3.2 Taking into account the nature of the Processing, IIJ shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

3.3 In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, IIJ shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent IIJ is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from IIJ's provision of such assistance.

4. IIJ PERSONNEL

4.1 IIJ shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. IIJ shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 IIJ shall take commercially reasonable steps to ensure the reliability of any IIJ personnel engaged in the Processing of Personal Data.

4.3 IIJ shall ensure that IIJ's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

4.4 Members of the IIJ Group have appointed a data protection officer. The appointed person may be reached at iijgroup-dpo-contact@iij.ad.jp .

5. SUB-PROCESSORS

5.1 Customer acknowledges and agrees that (a) IIJ's Affiliates may be retained as Sub-processors; and (b) IIJ and IIJ's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. IIJ and IIJ's Affiliates can engage another processor based on this DPA. Both IIJ and its Affiliates have in the past engaged and continue to engage multiple Sub-processors. The Sub-processors have been engaged by IIJ and its Affiliates at their own discretion and with only high data protection principles in mind. IIJ or an IIJ Affiliate have entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor. The Customer herewith confirms the engagement of the current Sub-processors, pursuant to the change-notification procedure as shown in this Sect. 5.

5.2 IIJ shall upon request make available to Customer the current list of Sub-processors for the Services identified based on the request by Customer. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location. IIJ shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services. Notifications of new Sub-processors shall be done via e-mail to an address dedicated by the Customer for this purpose as indicated on the signing page below.

5.3 Customer may object to IIJ's use of a new Sub-processor by notifying IIJ promptly in writing within ten (10) business days after receipt of IIJ's notice in accordance with the mechanism set out in Section 5.2. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, IIJ will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If IIJ is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by IIJ without the use of the objected-to new Sub-processor by providing written notice to IIJ. IIJ will only refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, in case the customer's objection against a new sub-processor is based on reasonable concerns regarding the particular sub-processor or IIJ and Customer agrees to a refund at the time of cancellation.

5.4 IIJ shall be liable for the acts and omissions of its Sub-processors to the same extent IIJ would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY

6.1 IIJ shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data,. IIJ regularly monitors compliance with these measures. IIJ will not materially decrease the overall security of the Services during a subscription term.

6.2 IIJ has obtained and may obtain in the future certain certification and security audits. Currently, IIJ has obtained certification by ISMS. A description of such certification can be found under https://www.iij.ad.jp/isms/ .

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

IIJ maintains security incident management policies and procedures and shall, notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by IIJ or its Sub-processors of which IIJ becomes aware (a "**Customer Data Incident**"). IIJ shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as IIJ deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within IIJ's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users. IIJ will not contact data subject directly, unless the controller is unable to do so itself, requests IIJ's assistance in notifying the data subject and IIJ has the reasonable means to make a notification on the controller's behalf.

8. RETURN AND DELETION OF CUSTOMER DATA

IIJ shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data adhering to internationally acceptable standards and without undue delay.

9. AUTHORIZED AFFILIATES

9.1 The parties acknowledges and agree that, by executing the Agreement, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between IIJ and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 9 and Section 10. Each

Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services and Content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer. The Customer is duly authorized to enter into this DPA in the name and on behalf of the respective authorized affiliate, referring to the SAMPLE OF POWER OF ATTORNEY (Schedule 2), and agrees to indemnify IIJ for any damages resulting from a lack of proper authorization.

9.2 The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with IIJ under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9.3 Where an Authorized Affiliate becomes a party to the DPA with IIJ, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

9.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against IIJ directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 9.3.2, below).

9.3.2 The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on- site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on IIJ and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

10. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and IIJ, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, IIJ's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

11. EUROPEAN SPECIFIC PROVISIONS

11.1 IIJ will process Personal Data in accordance with the GDPR requirements directly applicable to IIJ's provision of its Services.

11.2 Upon Customer's request, IIJ shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to IIJ. IIJ shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 11.2 of this DPA, to the extent required under the GDPR.

11.3 This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to IIJ for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately.

11.4 IIJ applies the following data transfer mechanisms for transfer of Personal Data from the European Union, the European Economic Area and/or their member states and Switzerland ("**EEA countries**") to non-EEA countries:

a. the adequacy decisions granted by the European Commission in pursuant to Article 45 of the GDPR for transfers of Personal Data from the EEA countries to non-EEA countries which are granted with such adequacy decision;

b. the IIJ Processor BCR to transfers of Personal Data (i) among IIJ Group members who act as Processor or Sub-processor, or (ii) from a Customer established in the European Economic Area member states or Switzerland whose processing activities for the relevant data are governed by the GDPR and/or implementing national legislation to an IIJ Group member who acts as a Processor, or (iii) from non-European Economic Area member states for which Customer has contractually specified that the GDPR and implementing national legislation shall apply, to an IIJ Group

member who acts as a Processor, or (iv) from an IIJ Group member who acts as a Processor to a non-IIJ Group Sub-processor located outside the European Economic Area; and

    c.   the SCC 2021 (set forth in Schedule 3 to this DPA) to transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states and Switzerland to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations; and

In the event that no adequacy decision as stated in Section 11.4(a) of this DPA is applicable and a transfer of Personal Data is covered by more than one transfer mechanism, the transfer of Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: (1) the IIJ Processor BCR, and (2) the SCC 2021.

11.5   IIJ applies the following data transfer mechanisms for transfer of Personal Data from the United Kingdom to other countries:

    a.   the adequacy regulations granted by the United Kingdom's Secretary of State under section 17A of the Data Protection Act 2018 of the United Kingdom for transfers of Personal Data from the United Kingdom to countries which are granted with such adequacy decision;

    b.   the SCC 2010 (set forth in Schedule 4 to this DPA) to transfers of Personal Data under this DPA from the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the United Kingdom, to the extent such transfers are subject to such Data Protection Laws and Regulations. IIJ reserves the right to update or replace the SCC 2010 in Schedule 4 with an equivalent international data transfer mechanism at any time in the effort to comply with the Data Protection Laws and Regulations of the United Kingdom. The Customer will be informed in advance by IIJ and be deemed to agree, if the Customer does not object to such update or replacement of Schedule 4 within ten (10) business days upon being informed.

11.6   Regardless of the origin of Personal Data, IIJ applies the IIJ Processor BCR to transfers of Personal Data from an IIJ Group member who acts as a Controller to an IIJ Group member who acts as a Processor.

11.7   The SCC 2010 and SCC 2021 apply to (i) the legal entity that has executed the SCC 2010 or SCC 2021 as a data exporter and its Authorized Affiliates and, (ii) all Affiliates of Customer established within the European Economic Area and Switzerland (for the SCC 2021) or the United Kingdom (for the SCC 2010), which have signed Order Forms for the Services. For the purpose of the SCC 2010 and SCC 2021, the aforementioned entities shall be deemed "data exporters".

11.8   This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to IIJ for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately.

12.   LEGAL EFFECT

This DPA shall only become legally binding between Customer and IIJ when the formalities steps set out in the Section "HOW TO EXECUTE THIS DPA" above have been fully completed.

<u>**List of Schedules**</u>

Schedule 1: Details of the Processing
Schedule 2: Sample of Power of Attorney
Schedule 3: Standard Contractual Clauses 2021
Schedule 4: Standard Contractual Clauses 2010

[CUSTOMER]

Signature:_____

Customer Legal Name:_____

Print Name:_____

Title:_____

Date:

E-mail address for notifications of this DPA including Art. 5.2 and Art. 7:

_____

Service Agreement etc.:

_____

[IIJ]

Signature:_____

Print Name:_____

Title:_____

Date:

SCHEDULE 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

IIJ will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services.

Duration of Processing

Subject to Section 8 of the DPA, IIJ will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's Users authorized by Customer to use the Services

Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localization data

Changes to the details of processing

In case of any changes in the data processing operations of the Customer, which directly affect the data processing carried out by IIJ on behalf of the Customer, the Customer shall notify IIJ of these changes without delay. In particular, the Customer shall notify IIJ of any changes regarding the types of personal data submitted to IIJ or the categories of data subjects affected by such processing as listed in this Schedule 1, 3 and 4.

SCHEDULE 2 – SAMPLE OF POWER OF ATTORNEY

Power of Attorney
The undersigned company
[name of entity who grants the PoA, i.e. the Authorized Affiliate]
(the "**Principal**"),

hereby authorizes
[name of other entity to whom the PoA is granted, i.e. the Customer to the DPA]
(the "**Authorized Person**"),

to represent the Principal in entering into the Data Processing Addendum and its Schedules ("**DPA**") with respect to the processing of personal data, dated [enter signing date of the DPA], between the Authorized Person and Internet Initiative Japan, Inc., Iidabashi Grand Bloom 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102-0071, JAPAN or any of its affiliates ("**IIJ**")

The Authorized Person is entitled to
1. issue all declarations which are necessary or expedient in connection with legal acts referred to above;
2. make use of this power of attorney in part and/or more than once, also in order to amend, supplement, terminate or approve declarations or statements already made under this power of attorney;
3. delegate to a third person, in full or in part, including by way of a comprehensive sub-power of attorney, any of the authorities granted pursuant to this power of attorney.

In case of doubt, this power of attorney shall be broadly interpreted so as to ensure that its economic purpose is achieved at all times.

    On behalf of the Principal:

_____   _____
Date   Name, Position

SCHEDULE 3 - STANDARD CONTRACTUAL CLAUSES 2021

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**")

    (each such Entity hereinafter a "**Party**")

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.

(e) Clauses 8, 9 and 10 are divided into modules varying depending on the data transfer relation between each Data Exporter and each Data Importer. In applying such Clauses:

    (i) if the Data Exporter is a controller and the Data Importer is a processor of the personal data under concern, only paragraphs under "**MODULE TWO: Transfer controller to processor**" are applicable; or

    (ii) if the Data Exporter and Data Importer are both processors of the personal data under concern, only paragraphs under "**MODULE THREE: Transfer processor to processor**" are applicable.

Paragraphs without a preceding module title shall be applicable to both modules.

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(a), (d) and (f);

 (v) Clause 13;

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

 (vii) Clause 16(e);

 (viii) Clause 18(a) and (b).

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

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

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

Clause 6
Description of the transfer(s)

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

Clause 7
Docking clause

(a) An Entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a Data Exporter or as a Data Importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding Entity shall become a Party to these Clauses and have the rights and obligations of a Data Exporter or Data Importer in accordance with its designation in Annex I.A.

(c) The acceding Entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The Data Exporter warrants that it has used reasonable efforts to determine that the Data Importer is able, through the implementation of appropriate technical and organizational 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 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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, 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 organizational 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 authorized 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 defense 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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, 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 organizational 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 authorized 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

15

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 defense 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

16

(a) The data importer has the data exporter's general authorization 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 ten (10) business 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 authorization 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 ten (10) business 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 authorized 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 organizational 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 authorized 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 organizational 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 authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the Data Importer shall accept the decision of the data subject to:

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

   (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organization 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 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 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 behavior is monitored, are located 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 authorizing 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

19

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 authorizing 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 organizational 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 organizational 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

20

(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 minimization

(a) The Data Importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The Data Importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the Data Importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the Data Importer under Clause 14(e).

(b) The Data Importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter. It shall also make it available to the competent supervisory authority on request. [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.

21

(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. The Data Importer shall certify the deletion of the data to the Data Exporter. Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred personal data, the Data Importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17
Governing law

These Clauses shall be governed by the law of 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 the

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 Frankfurt am Main, Germany.

(c) A data subject may also bring legal proceedings against the Data Exporter and/or Data Importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES 2021

A. **LIST OF PARTIES**

Data Exporter(s): Data Exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates (as defined in the Agreement) of Customer established within the European Union, the European Economic Area and Switzerland that have purchased the Services on the basis of one or more Order Form(s).

Data Importer(s): IIJ is a provider of enterprise cloud computing solutions which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons);
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors;
- Employees, agents, advisors, freelancers of data exporter (who are natural persons); and
- Data exporter's Users authorized by data exporter to use the Services.

Categories of personal data transferred

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localization data

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 specialized training), keeping a record of access to the data, restrictions for Onward Transfers or additional security measures.

Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

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

Subject to Section 8 of the DPA, IIJ will Process Personal Data on a continuous basis for the duration of the Agreement, unless otherwise agreed upon in writing.

Nature of the processing (what the Data Importer will do with the data transferred, e.g. storing, analyzing, contacting data subjects)

IIJ will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services.

Purpose(s) of the data transfer and further processing

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement.

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

Subject to Section 8 of the DPA, IIJ will Process Personal Data for the duration of the Agreement, unless there is any reasonable business reason or legal regulation or otherwise agreed upon in writing.

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

IIJ will further transfer Personal Data to third-party contractors which process Personal Data as sub-processors, so far as such sub-processing is necessary for the performance of the Services pursuant to the Agreement. Such third-party contractors discharge functions including, but not limited to, customer support, service monitoring, etc. Such third-party contractors retain Personal Data as long as sub-processing contracts are effective between IIJ and such contractors and such sub-processing is necessary for the performance of the Services.

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

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services. Data Importer will not materially decrease the overall security of the Services during a subscription term.

IIJ-BRM003-0004

SCHEDULE 4 - STANDARD CONTRACTUAL CLAUSES 2010

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation:

Address:

Tel.:   ; fax: ; e-mail:

Other information needed to identify the organisation:

……………………………………………………………
(the data **exporter**)

And

Name of the data importing organisation:

Address:

Tel.:   ; fax: ; e-mail:

Other information needed to identify the organisation: Not applicable

(the data **importer**)

Each "a party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) *'the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter
The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b)   that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c)   that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d)   that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e)   that it will ensure compliance with the security measures;

(f)   that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g)   to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h)   to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i)   that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j)   that it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer

The data importer agrees and warrants:

(a)   to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b)   that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c)   that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d)   that it will promptly notify the data exporter about:

    (i)   any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

    (ii)   any accidental or unauthorised access, and

    (iii)   any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e)   to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f)   at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members

and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1.   The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2.   The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.   The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4.   The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12
Obligation after the termination of personal data processing services

1.   The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2.   The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…………………………………….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…………………………………….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES 2010

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data Exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates (as defined in the Agreement) of Customer established the United Kingdom that have purchased the Services on the basis of one or more Order Form(s).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

IIJ is a provider of enterprise cloud computing solutions which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter's Users authorized by data exporter to use the Services

Categories of data

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localisation data

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement.

DATA EXPORTER

Name:…………………………….…

Authorised Signature ……………………

DATA IMPORTER

Name:…………………………….…

Authorised Signature ……………………

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES 2010

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services. Data Importer will not materially decrease the overall security of the Services during a subscription term.

DATA EXPORTER

Name: …………………………….…

Authorised Signature …………………

DATA IMPORTER

Name: …………………………….…

Authorised Signature …………………

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES 2010

The data exporter and importer hereto agree to the following provisions in addition to the Standard Contractual Clauses 2010

1. General and specific references in the Standard Contractual Clauses 2010 to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 shall hereby be deemed to have the same meaning as the equivalent reference in the Data Protection Laws and Regulations applicable in the United Kingdom.

2. References in the Standard Contractual Clauses 2010 to "the law of the Member State in which the data exporter is established" shall hereby be deemed to mean "the law of the United Kingdom".

3. Any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter is established shall hereby be deemed to refer to an obligation under Data Protection Laws and Regulations applicable in the United Kingdom.

4. For the purposes of Clause 5(a) of the Standard Contractual Clauses 2010, the following is deemed an instruction by the data exporter to process Personal Data: (a) Processing in accordance with the Agreement and applicable Order Form(s); (b) Processing initiated by Users in their use of the Services and (c) Processing to comply with other reasonable documented instructions provided by data exporter (e.g., via email) where such instructions are consistent with the terms of the Agreement.

5. Pursuant to Clause 5(h) of the Standard Contractual Clauses 2010, the data exporter acknowledges and expressly agrees that (a) the data importer's Affiliates may be retained as Sub-processors; and (b) the data importer and the data importer's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. The data importer shall make available to Customer the current list of Sub-processors.

6. Pursuant to Clause 5(h) of the Standard Contractual Clauses, data exporter acknowledges and expressly agrees that data importer may engage new Sub-processors as described in Sections 5.2 and 5.3 of the DPA.

7. The parties agree that the copies of the Sub-processor agreements that must be provided by data importer to data exporter pursuant to Clause 5(j) of the Standard Contractual Clauses 2010 may have all commercial information, or clauses unrelated to the Standard Contractual Clauses 2010 or their equivalent, removed by data importer beforehand; and, that such copies will be provided by data importer, in a manner to be determined at its discretion, only upon request by data exporter.

8. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses 2010 shall be carried out in accordance with the following specifications:

    Upon data exporter's request, and subject to the confidentiality obligations set forth in the Agreement, data importer shall make available to data exporter that is not a competitor of data importer (or data exporter's independent, third-party auditor that is not a competitor of data importer) information regarding the data importer's compliance with the obligations set forth in the DPA in the form of the third-party certifications and audits to the extent data importer makes them generally available to its customers. Data exporter may contact data importer in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Data exporter shall reimburse data importer for any time expended for any such on-site audit at the data importer's then-current professional services rates, which shall be made available to data exporter upon request. Before the commencement of any such on-site audit, data exporter and data importer shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which data exporter shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by data importer. Data exporter shall promptly notify data importer with information regarding any non- compliance discovered during the course of an audit.

9. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses 2010 shall be provided by data importer to data exporter only upon data exporter's request.

10. In the event of any conflict or inconsistency between the body of the DPA and any of its Schedules (not including the Standard Contractual Clauses 2010) and this Standard Contractual Clauses 2010, the Standard Contractual Clauses 2010 shall prevail.

DATA EXPORTER

Name:…………………………………

Authorised Signature: ……………………

DATA IMPORTER

Name:…………………………………

Authorised Signature: ……………………