

Supplier Data Processing Addendum

This Supplier Data Processing Addendum ("DPA") is effective as of the effective date and forms part of the Contract for Services ("Principal Agreement") between Virtusa (Company) and _____ (Data Processor)

"Data Processor"	Full legal name: Country of Incorporation: Postal address: Email address:
"Company"	Full legal name: [insert full legal name of Virtusa entity benefitting from the contract e.g. Virtusa Consulting & Services Limited] Country of Incorporation: Postal address: [insert address e.g. 26 Finsbury Square, Level 8, London EC2A 1DS] Email address:
"Effective Date"	The date this DPA is signed by Virtusa.
"Term"	This DPA will start on the effective date and continue until terminated.

WHEREAS

(A) The Company acts as a Data Controller.

(B) The Company wishes to contract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing addendum that complies with the requirements of the current legal framework in relation to data processing and with 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).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this addendum shall have the following meaning:

1.1.1 "Addendum" means this Data Processing Addendum and all Schedules;

1.1.2 "Company Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 "Contracted Processor" means a Processor appointed by the Data Controller;

1.1.4 "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "EEA" means the European Economic Area;

1.1.6 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "GDPR" means EU General Data Protection Regulation 2016/679;

1.1.8 "Data Transfer" means:

1.1.8.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments/ affiliates of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "Services" means _____ for the company.

Commented [KP1]: To be updated by the vendor/
business team

1.1.10 "Sub processor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the addendum.

1.1.11 "Applicable Laws" means shall mean the relevant data protection and privacy law, regulations (including EU GDPR and the UK GDPR) and other regulatory requirements to which Virtusa are subject, and any guidance or statutory codes of practice issued by the relevant Privacy Authority/ies.

1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing", "Data Protection Impact Assessment" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company's documented instructions, unless required to do so by EU Data Protection Laws to which the Contracted Processor is subject; in such a case, the Contracted Processor shall inform the Company of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest

2.2 The Company instructs Contracted Processor to process Company Personal Data.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Company and Contracted Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Sub-Processing

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless required or authorized by the Company. Such Subprocessor shall be subject to the same level of data protection and security as under this Agreement. Data Importer is responsible for the performance of the Data Importer's Affiliates' and Third-Party Subprocessor' obligations in compliance with the terms of this Data Processing Agreement and Applicable Data Protection Law.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are requested by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and prior consultation, Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data, unless EU Data Protection Laws requires storage of the personal data.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Company on reasonable request all information necessary to demonstrate compliance with this addendum, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Contracted Processors, provided that Company shall give reasonable notice to the Provider prior to conducting such audit.

10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the addendum does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

10.3 The terms of such audit or inspection shall be clearly defined and agreed upon by both Company and Processor, Company and its designee proposing to undertake an audit shall give reasonable notice to the Processor of any audit or inspection to be conducted under section 10.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. Audit or inspections must be carried out in the presence of an officer / personnel designated by the Processor.

10.4 Processor is not required to give access to its premises for the purposes of such an audit or inspection:

- a) to any individual who fails to produce reasonable evidence of identity and authority;
- b) outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Company or its relevant undertaking an audit has given notice to Provider or its relevant Affiliate that this is the case before attendance outside those hours begins;
- c) if the inspection infringes upon Provider's Intellectual Property or compliance with Data Protection Agreements that Provider may have with its other partners or customers;

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this addendum is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 Confidentiality. Each Party must keep this addendum and information it receives about the other Party and its business in connection with this addendum ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

- (a) disclosure is required by law;
- (b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this addendum must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this addendum at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This addendum is governed by the laws of India.

13.2 Any dispute arising in connection with this addendum, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Hyderabad.

IN WITNESS WHEREOF, this agreement is entered into with effect from the date first set out below.

Virtusa

Data Processor name

Signature _____
Name: _____

Signature : _____
Name: _____

Title: _____
Date Signed: _____

Title: _____
Date Signed: _____

APPENDIX 1 TO THE DATA PROCESSING ADDENDUM

Commented [KP2]: To be updated by the vendor/
business team

DETAILS OF THE PROCESSING

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 **Virtusa**, a information technology services company, which requires the services of _____, the data importer.

Data importer

The data importer is _____ and will assist **Virtusa** in a range of services (as detailed below)

Data subjects

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

Categories of data

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

Special categories of data (if appropriate)

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

Processing operations

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

Data Processor: **Virtusa**

Data Processor:

Name:.....

Name:.....

Authorised Signature

Authorised Signature

APPENDIX 2 TO THE DATA PROCESSING ADDENDUM

Description of the technical and organizational security measures implemented as a minimum by the Data Processor in accordance with Section 4 of the Data Processing Addendum and are in addition the security requirements and related policies as per the Agreement. This Appendix 2 forms an integral part of the Data Processing Addendum

1. The Processor shall bring into effect and maintain appropriate technical and organizational measures to prevent unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The Processor shall at a minimum implement and maintain the following technical and organizational security measures to protect personal data against unauthorized or unlawful processing, accidental or unlawful destruction or accidental loss, alteration, damage, and unauthorized disclosure:
 - (a) adopt and implement policies and standards related to information security;
 - (b) assign responsibility for information security management;
 - (c) devote adequate personnel resources to information security;
 - (d) perform background checks on staff that will have access to the personal data (where practicable and lawful in each relevant jurisdiction);
 - (e) require its employees, staff, vendors and others to abide by its information security standards and other privacy policies (as such may be revised from time to time), which standards and policies include confidentiality provisions;
 - (f) conduct training to make employees aware of information security risks and to enhance compliance with its policies and standards relating to the protection of personal data;
 - (g) have procedures in place in order to prevent unauthorized access to personal data through the use, as appropriate, of physical and logical (password) entry controls, secure areas for processing, procedures for monitoring the use of processing facilities, and built in system audit trails;
 - (h) protect the personal data maintained in online systems through the use, as appropriate, of secure passwords, network intrusion prevention and detection technology, encryption and authentication technology, secure log on procedures, and virus protection; and
 - (i) ensure compliance with its policies and standards related to the protection of the personal data on an ongoing basis.
2. Without prejudice to the foregoing, the technical and organizational security measures shall include the following:
 - (a) physical security policies and procedures consisting of: (i) restricted access to areas where personal data may be located or accessed; (ii) installation of closed circuit television cameras strategically placed in areas where personal data may be located or accessed; and (iii) appropriate fire detection and fire suppression systems intended to maximize early detection to avoid sprinkler deployment; and
 - (b) electronic security policies and procedures consisting of: (i) firewalls restricting access to servers containing personal data that are connected to a public network; and (ii) appropriate encryption and security practices to prevent unauthorized or unlawful processing of personal data and to prevent accidental loss or destruction of, or damage to, personal data.
3. Further, and without prejudice to the foregoing, the Processor agrees to implement the following minimum technical security measures:
 - (a) measures taken to prevent any unauthorized person from accessing the facilities used for data processing (monitoring of entry to facilities);

- (b) measures taken to prevent data media from being read, copied, amended or moved by any unauthorized persons (monitoring of media);
 - (c) measures taken to prevent the unauthorized introduction of any data into the information system, as well as any unauthorized knowledge, amendment or deletion of the recorded data (monitoring of memory);
 - (d) measures taken to prevent data processing systems from being used by unauthorized person using data transmission facilities (monitoring of usage);
 - (e) measures taken to guarantee that authorized persons when using an automated data processing system may access only data that are within their competence (monitoring of access);
 - (f) measures taken to guarantee the checking and recording of the identity of third parties to whom the data can be transmitted by transmission facilities (monitoring of transmission);
 - (g) measures taken to guarantee that the identity of the persons having had access to the information system and the data introduced into the system can be checked and recorded ex post facto at any time and by any person (monitoring of introduction);
 - (h) measures taken to prevent data from being read, copied, amended or deleted in an unauthorized manner when data are disclosed and data media transported (monitoring of transport); and
 - (i) measures taken to safeguard data by creating backup copies (monitoring of availability).
4. At the request of the Controller, the Processor shall, within ten (10) calendar days of the date of the Controller's request, provide to the Controller a detailed description (in the form specified by the Processor) of the security measures implemented in accordance with this Schedule 2 and shall inform the Controller without undue delay of any material changes impacting the above security measures throughout the term of the Agreement.
 5. The Processor shall allow the Controller, and any employees, agents, auditors or regulators of that Processor (collectively, the Approved Parties), to access and inspect: (a) the personal data of the Controller; and (b) the Processor's data processing facilities, procedures and documentation which relate to the processing of personal data to the extent necessary for the Controller (or any Approved Party) to ascertain the Processor's compliance with the terms of this Schedule 2 and any other term of the Clauses. The Processor shall co-operate with the Controller and the Approved Parties in the carrying out of such audits. Without prejudice to the foregoing and upon any Controller's written request, the Processor shall provide the Controller with written evidence of the Processor's compliance with the provisions of this Schedule 2 and any other term of the Agreement.
 6. For the avoidance of doubt, the Processor must ensure that any further processor (i) implements security measures complying with the requirements of the Data Processing Supplement and (ii) complies with the obligation to provide a detailed description (in the form specified by the Processor) of the security measures implemented within ten (10) calendar days from the Processor's request.

Data Controller: Virtusa

Name:.....

Authorised Signature

Data Processor:

Name:.....

Authorised Signature

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)¹ for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies

(hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)

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.

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

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 One: Clause 8.5 (e) and Clause 8.9(b); 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); Module Four: Clause 8.1 (b) and Clause 8.3(b);
- (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
- (iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
- (v) Clause 13;
- (vi) Clause 15.1(c), (d) and (e);
- (vii) Clause 16(e);
- (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4

Interpretation

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union⁽⁴⁾ (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

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

Clause 9 ***Use of sub-processors***

MODULE TWO: Transfer controller to processor

(a) **OPTION 1: SPECIFIC PRIOR AUTHORISATION** The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [Specify time period] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer

shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.(8)The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their

rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

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

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body² at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

MODULE TWO: Transfer controller to processor

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

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

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

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

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

² The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

- (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

MODULE TWO: Transfer controller to processor

- (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

MODULE TWO: Transfer controller to processor

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

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

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

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries,

submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination—including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards³;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data

³ As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or

exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Notification

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

- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of

destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

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

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

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules.

These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

- (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
- (ii) the data importer is in substantial or persistent breach of these Clauses; or
- (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] 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

MODULE TWO: Transfer controller to processor

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

[OPTION 2 (for Modules Two and Three): 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 _____ (*specify Member State*).]

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(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 _____ (*specify Member State*).

- (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

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

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

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

2. ...

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

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

2. ...

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

.....

Categories of personal data transferred

.....

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

.....

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

.....

Nature of the processing

.....

Purpose(s) of the data transfer and further processing

.....

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

.....

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

.....

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

.....

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

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

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

The controller has authorised the use of the following sub-processors:

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...

2. ...

ANNEX IV – ADDITIONAL APPLICABLE PRIVACY PROVISIONS

The following provisions will apply if and to the extent applicable to the Processing of Virtusa Personal Data by _____the vendor.

1. CCPA

1.1. To the extent _____vendor is a “Service Provider” (as defined under CCPA) and receives Virtusa Personal Data that constitutes “personal information” (as defined under CCPA) (“Personal Information”), _____vendor, in its role as a Service Provider, shall not (i) “sell” (as defined under CCPA) such Personal Information; (ii) retain, use, or disclose such Personal Information for any purpose other than performing the Services under the Agreement or as otherwise permitted under CCPA; (iii) retain, use, or disclose the Personal Information for a commercial purpose other than providing the Services unless otherwise permitted under the Agreement; or (iv) retain, use, or disclose such Personal Information outside of the direct business relationship between Virtusa and Service Provider unless otherwise permitted under the Agreement. _____Vendor, in its role as a Service Provider, agrees to comply with the CCPA as applicable to Service Provider in its provision of the Services to Virtusa under the Agreement.

1.2. In the event of any conflict between the terms of this Section 1 of Annex IV and any other terms of the DPA, the terms in this Section 1 of Annex IV shall control but only to the extent they apply to handling of Personal Information.

2. United Kingdom (“UK”) specific provisions

2.1. If and to the extent that the GDPR, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, (“UK GDPR”) or the UK Data Protection Act 2018 (collectively with the UK GDPR known as “UK Data Protection Law”), in each case as applicable in the UK, applies in relation to any Virtusa Personal Data:

2.1.1. any references in the DPA to the GDPR and its provisions shall be construed as referring instead to the equivalent sections of the UK Data Protection Law and its corresponding provisions;

2.1.2. any references in the DPA to European Union Member State Law shall be construed as references to applicable UK law;

2.1.3. any references in the DPA to the EEA and/or the EU shall be construed as references to the UK; and

2.1.4. any references in the DPA to the European Commission shall be construed as references to the UK Government.

2.2. If and to the extent that the UK Data Protection Law applies in relation to any Virtusa Personal Data and UK Data Protection Law requires a Cross-Border Transfer Mechanism for transfers of that Virtusa Personal Data, that occur either directly from the UK or outside the UK via onward transfer to a recipient located in a country not recognized by the UK as providing an adequate level of protection for Personal Data (“UK Transfers”), the transfers shall be safeguarded by the UK Standard Contractual Clauses, incorporated by reference to this DPA (including its constituent elements set forth in Schedule 1 of this DPA), unless Virtusa adopts another legally valid Cross-Border Transfer Mechanism, in Virtusa’s sole discretion and to the extent permitted by Data Protection Laws. For the purpose of this paragraph, the term “UK Standard Contractual Clauses” shall mean the 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, as approved by the European Commission in Decision 2010/87/EU, and/or any successor to such clauses adopted by the UK from time to time. Virtusa will take on the obligations of the “data exporter” for purposes of the UK Standard Contractual Clauses and _____ Vendor will take on the obligations of the “data importer” for purposes of the UK Standard Contractual Clauses.