Vendor DATA PROTECTION TERMS AND CONDITIONS

This Data Protection Terms and Conditions are applicable to all parties signing the Principle Agreement or SOW or Purchase order to be a partner (Vendor or acting as agent for each Vendor Affiliate and on its own behalf) with RPS Consulting Ltd. (Company or legal entity to be included here, hereinafter referred as "RPS ") acting on as agent for each Company Affiliate and on its own behalf.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added to the Principal Agreement or SOW or Purchase order as an Addendum. Except where the context requires otherwise, references in this Addendum to the Principal Agreement or SOW or Purchase Order are to the Principal Agreement or SOW or Purchase Order as amended by, and including, this Addendum.

These terms and conditions shall become effective when the Principle Agreement or SOW or Purchase order is signed between the parties.

RECITALS

Vendor, will perform Scope under the Principle Agreement or SOW or Purchase order, which provides for the Processing of Personal Data.

Vendor agrees to comply with the terms in this Addendum in the performance of SCOPE under the Principle Agreement or SOW or Purchase order.

1.   Definitions

1.1   In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

  1.1.1   **Applicable Laws** means

    (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and

    (b) any other applicable law with respect to any Company Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;

  1.1.2   **Annexures Applicability** means

    (a) If RPS collects any information of EU/EEA data subjects and transferring such data to sub-contractor/third party vendor, then **APPENDIX I - Exhibit A**: EU Controller-to-Processor Standard Contractual Clauses applicable.

    (b) If RPS sub-contracts/ third party vendor for processing the information of EU/EEA data subjects, then **APPENDIX I - Exhibit B:** EU Processor-to-Processor Standard Contractual Clauses applicable.

    (c) If sub-contractor/third party vendor collects any information of EU/EEA data subjects on behalf of RPS, then **APPENDIX I - Exhibit C**: Processor-to-Controller applicable.

(d) For sub-contractor/third party vendors outside EU/EEA/U.K. region **APPENDIX II: Technical & Organizational Measures** will be applicable to them.

(e) If RPS

    - collects any information of UK data subjects and transferring such data to sub-contracted/third party vendor;

    - sub-contracts/ third party vendor for processing the information of U.K. data subjects;

    - sub-contractor/third party vendor collects any information of U.K. data subjects on behalf of RPS,

then **APPENDIX III: U.K. SCC Clauses** will be applicable.

1.1.3   **Company Affiliate** means

an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.4   **Company Group Member** means

Company or any Company Affiliate;

1.1.5   **Company Personal Data** means

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

1.1.6   **Contracted Processor** means

Vendor or a Sub processor;

1.1.7   **Data Exporter** means

The controller who transfers the personal data.

1.1.8   **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.

1.1.9   **UK Data Protection Laws** means

the UK Data Protection Act 2018, UK GDPR and any associated regulations or instruments implementing or supplementing UK Data Protection Laws;

1.1.10   **Data Subject** means

Any person whose Personal Information (PI) and Sensitive Personal Information (SPI) are being gathered, stored or processed able to identify directly or indirectly natural person.

Respective SCC Clauses are only applicable, if any one of the below conditions satisfy:

(i) data of EU citizens are transferred/gathered; and/or

(ii) data of U.K. citizens are transferred/gathered.

1.1.11 **EEA** means

the European Economic Area;

1.1.12 **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;

1.1.13 **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);

1.1.14 **Restricted Transfer** means:

1.1.14.1 a transfer of Company Personal Data from any Company Group Member to a Contracted Processor; or

1.1.14.2 an onward transfer of Company Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments 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) in the absence of the Standard Contractual Clauses to be established under section [6.4.3 or] 12 below;

1.1.15 **Services** means

the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company Group Members pursuant to the Principal Agreement;

1.1.16 **Standard Contractual Clauses** means

the contractual clauses for the purposes of the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection. Amended in 2021

1.1.17 **Sub processor**

means any person (including any third party and any Vendor Affiliate, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor or any

Vendor Affiliate to Process Personal Data on behalf of any Company Group Member in connection with the Principal Agreement; and

1.1.18 **Supervisory Authority** means

an independent public authority which is established by an EU Member State pursuant to the GDPR.

1.1.19 **U.K. Addendum** means

the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers as adopted from time to time by the UK Information Commissioners Office in accordance with Article 46(2) of the UK GDPR;

1.1.20 **U.K. GDPR** means

United Kingdom General Data Protection Regulation, 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;

1.1.21 **Vendor Affiliate** means

an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Vendor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.22 **Data Protection Laws** means

UK Data Protection Laws, EU Data Protection Laws and any other data protection laws, regulations, regulatory requirements and codes of practice applicable to the Vendor's and its affiliate's provision of the Services.

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

1.3 The word **include** shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority

Vendor warrants and represents that, before any Vendor Affiliate Processes any Company Personal Data on behalf of any Company Group Member, Vendor's entry into this Addendum as agent for and on behalf of that Vendor Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Vendor Affiliate.

3. Processing of Company Personal Data

3.1 Vendor and each Vendor Affiliate shall:

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

3.1.2   not Process Company Personal Data other than on the relevant Company Group Member's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Vendor or the relevant Vendor Affiliate shall to the extent permitted by Applicable Laws inform the relevant Company Group Member of that legal requirement before the relevant Processing of that Personal Data.

3.2   Each Company Group Member:

3.2.1   instructs Vendor and each Vendor Affiliate (and authorises Vendor and each Vendor Affiliate to instruct each Sub processor) to:

3.2.1.1   Process Company Personal Data; and

3.2.1.2   in particular, transfer Company Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement; and

3.2.2   warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 3.2.1 on behalf of each relevant Company Affiliate.

4.   Vendor and Vendor Affiliate Personnel

Vendor and each Vendor Affiliate 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.

5.   Security

5.1   Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Vendor and each Vendor Affiliate 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.

5.2   In assessing the appropriate level of security, Vendor and each Vendor Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

6.   Sub processing

6.1   Each Company Group Member authorises Vendor and each Vendor Affiliate to appoint (and permit each Sub processor appointed in accordance with this section 6 to appoint) Sub processors in accordance with this section 6 and any restrictions in the Principal Agreement.

6.2   Vendor and each Vendor Affiliate may continue to use those Subprocessors already engaged by Vendor or any Vendor Affiliate as at the date of this Addendum, subject to Vendor and each Vendor Affiliate in each case as soon as practicable meeting the obligations set out in section 6.4.

6.3   Vendor shall give Company prior written notice of the appointment of any new Sub-processor, including full details of the Processing to be undertaken by the Sub-processor. If, within [15 days] of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment:

Alternative A:

[Neither Vendor nor any Vendor Affiliate shall appoint (or disclose any Company Personal Data to) that proposed Sub processor until reasonable steps have been taken to address the objections raised by any Company Group Member and Company has been provided with a reasonable written explanation of the steps taken.]

Alternative B:

6.3.1   [Vendor shall work with Company in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub processor; and

6.3.2   where such a change cannot be made within [15 days] from Vendor's receipt of Company's notice, notwithstanding anything in the Principal Agreement, Company may by written notice to Vendor with immediate effect terminate the Principal Agreement to the extent that it relates to the Services which require the use of the proposed Sub processor.]

Alternative C:

[Neither Vendor nor any Vendor Affiliate shall appoint (nor disclose any Company Personal Data to) the proposed Sub processor except with the prior written consent of Company.]

6.4   With respect to each Sub processor, Vendor or the relevant Vendor Affiliate shall:

6.4.1   before the Sub processor first Processes Company Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the Sub processor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement;

6.4.2   ensure that the arrangement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Sub processor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

6.4.3   if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Sub processor; and on the other hand the Sub processor, or before the Sub processor first Processes Company Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Company Group Member(s) (and Company shall procure that each Company Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution); and

6.4.4   provide to Company for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Company may request from time to time.

6.5   Vendor and each Vendor Affiliate shall ensure that each Sub processor performs the obligations under sections 3.1, 4, 5, 7.1, 8.2, 9 and 11.1, as they apply to Processing of Company Personal Data carried out by that Sub processor, as if it were party to this Addendum in place of Vendor.

7.   Data Subject Rights

7.1   Taking into account the nature of the Processing, Vendor and each Vendor Affiliate shall assist each Company Group Member by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2   Vendor shall:

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

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

8.   Personal Data Breach

8.1   Vendor shall notify Company without undue delay upon Vendor or any Sub processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws. If you have any questions regarding our Privacy Statement or if you need to update, change, or remove information, you can do so by mailing at **<nimesh.aggarwal@rpsconsulting.in>** Immediately.

8.2   Vendor shall co-operate with Company and each Company Group Member and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9.   Data Protection Impact Assessment and Prior Consultation

Vendor and each Vendor Affiliate shall provide reasonable assistance to each Company Group Member 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 of any Company Group Member 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.

10.   Deletion or return of Company Personal Data

10.1   Subject to sections 10.2 and 10.3 Vendor and each Vendor Affiliate shall promptly and in any event within [2 months] 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.

10.2   Subject to section 10.3, Company may in its absolute discretion by written notice to Vendor within [7 days] of the Cessation Date require Vendor and each Vendor Affiliate to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Vendor; and (b) delete and procure the deletion of all other copies of Company Personal Data

Processed by any Contracted Processor. Vendor and each Vendor Affiliate shall comply with any such written request within [30 Days] of the Cessation Date.

10.3   Each Contracted Processor may retain Company Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vendor and each Vendor Affiliate shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

10.4   Vendor shall provide written certification to Company that it and each Vendor Affiliate has fully complied with this section 10 within [2 months] of the Cessation Date.

11.   Audit rights

11.1   Subject to sections [11.2 to 11.4], Vendor and each Vendor Affiliate shall make available to each Company Group Member on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by any Company Group Member or an auditor mandated by any Company Group Member in relation to the Processing of the Company Personal Data by the Contracted Processors.

11.2   Information and audit rights of the Company Group Members only arise under section 11.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

11.3   [Company or the relevant Company Affiliate undertaking an audit shall give Vendor or the relevant Vendor Affiliate reasonable notice of any audit or inspection to be conducted under section 11.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

  11.3.1   to any individual unless he or she produces reasonable evidence of identity and authority;

  11.3.2   outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Company or the relevant Company Affiliate undertaking an audit has given notice to Vendor or the relevant Vendor Affiliate that this is the case before attendance outside those hours begins; or

  11.3.3   for the purposes of more than [one] audit or inspection, in respect of each Contracted Processor, in any [calendar year], except for any additional audits or inspections which:

    11.3.3.1   Company or the relevant Company Affiliate undertaking an audit reasonably considers necessary because of genuine concerns as to Vendor's or the relevant Vendor Affiliate's compliance with this Addendum; or

    11.3.3.2   A Company Group Member is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

  where Company or the relevant Company Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Vendor or the relevant Vendor Affiliate of the audit or inspection.]

12.   Restricted Transfers

12.1   Subject to section 12.3, each Company Group Member (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Company Group Member to that Contracted Processor.

12.2   The Standard Contractual Clauses shall come into effect under section 12.1 on the later of:

12.2.1   the data exporter becoming a party to them;

12.2.2   the data importer becoming a party to them; and

12.2.3   commencement of the relevant Restricted Transfer.

12.3   Section 12.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12.4   [Vendor warrants and represents that, before the commencement of any Restricted Transfer to a Sub processor which is not a Vendor Affiliate, Vendor's or the relevant Vendor Affiliate's entry into the Standard Contractual Clauses under section 12.1, and agreement to variations to those Standard Contractual Clauses made under section 13.4.1, as agent for and on behalf of that Sub processor will have been duly and effectively authorised (or subsequently ratified) by that Sub processor.]

13.   General Terms

Governing law and jurisdiction

13.1   Without prejudice to clauses 17 (Governing Laws) and 18 (Choice of forum and jurisdiction) of the Standard Contractual Clauses:

13.1.1   the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2   this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Order of precedence

13.2   Nothing in this Addendum reduces Vendor's or any Vendor Affiliate's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Vendor or any Vendor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.3   Subject to section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

13.4   Company may:

13.4.1   by at least [30 (thirty) calendar days'] written notice to Vendor from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 12.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

13.4.2   propose any other variations to this Addendum which Company reasonably considers to be necessary to address the requirements of any Data Protection Law.

13.5   If Company gives notice under section 13.4.1:

13.5.1   [Vendor and each Vendor Affiliate shall promptly co-operate (and ensure that any affected Sub processors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place under section 6.4.3; and]

13.5.2   Company shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Vendor to protect the Contracted Processors against additional risks associated with the variations made under section 13.4.1 [and/or 13.5.1].

13.6   If Company gives notice under section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Company's notice as soon as is reasonably practicable.

13.7   Neither Company nor Vendor shall require the consent or approval of any Company Affiliate or Vendor Affiliate to amend this Addendum pursuant to this section 13.5 or otherwise.

Severance

13.8   Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Standard Contractual Clauses

[These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under the GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law (otherwise).] [If these Clauses are not governed by the law of a Member State, the terms "Member State" and "State" are replaced, throughout, by the word "jurisdiction".]

This document was updated on October 1, 2024

Standard Contractual Clauses (processors) - For the purposes of the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection.

Both Company and Vendor 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.

APPENDIX-I

EXHIBIT A: EU CONTROLLER-TO-PROCESSOR STANDARD CONTRCTUAL CLAUSES

Section I

Clause 1

Purpose and scope

(a)   The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b)   The Parties:

    (i)   the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

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

    have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c)   These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d)   The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a)   These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679,

provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b)   These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a)   Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i)   Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii)   Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii)   Clause 9(a), (c), (d) and (e);

(iv)   Clause 12(a), (d) and (f);

(v)   Clause 13;

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

(vii)   Clause 16(e); and

(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

Module II: Transfer Controller to Processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a)   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 prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

(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

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

(b)   The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

Clause 11

Redress

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

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body 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.

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

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

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

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

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

(e)   The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f)   The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a)   Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b)   The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c)   Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d)   The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e)   Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f)   The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g)   The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

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

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has

appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

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

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii)   any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c)   The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

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

(e)   The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). 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, 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 the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1   Notification

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

(i)   receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

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

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.). 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. 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.

<div align="center">

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

</div>

(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 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 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 Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b)   The Parties agree that those shall be the courts of (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.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: RPS Consulting Ltd and its affiliates

Address: As per Agreement/Statement of Work/ Purchase Order

Activities relevant to the data transferred under these Clauses: Agreement/Statement of Work/ Purchase Order

Role: Controller/Processor

Data importer(s): [*As per Agreement/Statement of Work/ Purchase Order*]

Name: ....

Address: ....

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

Role: Controller/Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose Personal Data is transferred	Individuals of whom Personal Data is Processed by or on behalf of the Data Exporter
Categories of Personal Data transferred	Categories of Personal Data (including sensitive Personal Data) transferred would be data, that, in connection with the performance of Processing services under the Agreement/Statement of Work/ Purchase Order
Restrictions or safeguards for personal data including sensitive data:	Safeguards implemented to tranfer Personal Data are as stated in Annex II- Technical and Organizational Measures
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	As necessary for Data Importers provision of Processing servicing and performance of its obligations under the Agreement/Statement of Work/ Purchase Order
Nature of the Processing	The nature of the Processing activity will be that as necessary for Data Importer's provision of the Processing activities and performance of its obligations under these Agreement/Statement of Work/ Purchase Order.
Purpose(s) of the data transfer and further Processing	Data Importer will Process European Personal Data in accordance with the terms of the Agreement/Statement of Work/ Purchase Order, for the purpose of performing the services under the Agreement/Statement of Work/ Purchase Order.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period	For the duration of the Agreement/Statement of Work/ Purchase Order pursuant to which the Data Importer will provide its Services to RPS, and thereafter as necessary to comply with applicable laws or contractual obligations.
For transfers to (sub-) processors, specify subject matter, nature and duration of the processing	As stated in Annex III

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13	The supervisory authority identified by the data exporter or as required by any local law.

This document was updated on October 1, 2024

ANNEX II

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

Vendor shall implement measures designed to:

- deny unauthorized persons access to data-processing equipment used for processing Personal Data(equipment access control);
- prevent the unauthorized reading, copying, modification or removal of data media (data media control);
- prevent the unauthorized input of Personal Data and the unauthorized inspection, modification ordeletion of stored Personal Data (storage control);
- prevent the use of automated data-processing systems by unauthorized persons using data communication equipment (user control);
- ensure that persons authorized to use an automated data-processing system only have access to thePersonal Data covered by their access authorization (data access control);
- ensure that it is possible to verify and establish to which individuals Personal Data have been or may be transmitted or made available using data communication equipment (communication control);
- ensure that it is subsequently possible to verify and establish which Personal Data have been put intoautomated data-processing systems and when and by whom the input was made (input control);
- prevent the unauthorized reading, copying, modification or deletion of Personal Data during transfers ofthose data or during transportation of data media (transport control);
- ensure that installed systems may, in case of interruption, be restored (recovery);
- ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored Personal Data cannot be corrupted by means of a malfunctioning of the system (integrity).

Vendor shall comply with the below mentioned Information Security Measures

- Set direction for and show commitment to information security. At a minimum there shall be a high-level information security policy and supporting program that applies enterprise-wide.
- Information shall not be excessively stored, printed, copied, disclosed or Processed by other meansoutside the purpose for use.
- Information shall be processed and stored logically separated from the Vendors own information and from that of other customers.
- Upon conclusion or termination of Vendor's work for RPS, the Vendor shall sanitize and securely destroy (or at RPS's election return to RPS) all copies of all Information, including all backup and archival copies, in any electronic or non-electronic form.
- Access to Information shall be restricted to Personnel individually and on a need to know basis.
- Access to information needs to be on individual basis and at least password protected, and computerscreens need to be locked in case of absence.
- Storage media containing Personal or Information shall be encrypted during transport and destroyedin a secure way.
- Records shall be kept in an auditable manner showing which Information has been has beenaccessed, modified, disclosed or disposed.
- Cryptographic controls shall be used in compliance with all relevant agreements,

legislation andregulations.

- Physical access to Vendor buildings shall be restricted to Personnel individually and on a need to have basis.
- Systems containing Information shall be protected by firewall(s) and properly hardened, i.e. removing or disabling software and functionalities that are not being used.
- Vendor networks used to access Information or networks shall have security controls that can protect against unauthorized traffic interception or interference by making use of firewalls, intrusiondetection/prevention, etc.
- Wireless network connections transferring Information shall be encrypted according to bestpractice.
- Vendor shall deploy technology to scan Vendor's corporate email for viruses and malicious code

  and links and keep such technology up to date.
- Disclosing Information to a third party, such as a Third-Party Sub-Processor, shall only be allowed with prior written consent from and only for the purposes identified in contractual agreements withRPS.
- Third Party Sub-Processors shall be restricted to only the necessary access, use, retention and disclosure of Information needed to fulfil contractual obligations.
- Third Party Sub-Processors shall be given clear instructions on security measures for protecting Information.
- Vendor shall have a documented security incident management process to detect and handle incidents. Vendor shall report confirmed security incidents or weaknesses involving Information or Services for as soon as practicable or as otherwise agreed upon.
- Security related incidents should be reported to: <nimesh.aggarwal@rpsconsulting.in>, appointed point of contact or as otherwise specified in contractual agreements.

- Vendor shall cooperate fully with in dealing with these reports. Cooperation may include providingaccess to computer-based evidence data for forensic evaluation.

Vendor shall comply with the below mentioned Data Privacy Measures

- Set direction for and show commitment to privacy. At a minimum there shall be a high-level privacy policy that applies enterprise-wide and assignment of overall responsibility for privacy to a top-level executive or equivalent.
- Vendor shall ensure protection and privacy of Personal Data related to Services in accordance with relevant data protection legislation and regulations.
- Personal Data, including redacted or Anonymized Personal Data, shall not be used for any other purposethan meeting Principle agreements or SOW or Purchase order with RPS.
- Personal Data collected for different purposes shall be processed separately.
- Personal Data shall not be accessed without prior authorization.
- Authorized Personnel shall only have access to the least amount of Personal Data to carry out their job duty.
- Personnel with access to Personal Data shall be required to take appropriate data privacy training on a regular basis.
- Personal Data shall be retained for only as long as necessary to fulfill the stated purposes in Principle Agreements or SOW or Purchase order with RPS, or as required by law or regulations, and shall thereafter be appropriately returned or disposed at the choice of RPS.
- The disposal of Personal Data shall be recorded to certify to that such disposal has taken place.
- Where the return or disposal of some, or all of the Personal Data is prevented by law or regulation, the Personal Data shall be kept confidential or anonymized and shall no longer

be processed shall be informed if such obligations exist immediately when Vendor becomes aware of them.

- Personal Data shall not be excessively stored, printed, copied, disclosed or other means of Processing outside the purpose for use.
- The Data Subject shall be provided with access to his or her Personal Data for review.
- In the event the Data Subject does not have direct access to his or her Personal Data, the Personal Data shall be transferred to in order to support any Data Subject request, without answering the request unless authorized to do so.
- Inaccurate Personal Data shall be corrected when the Data Subject or on the Data Subject's behalf, has

  made a request for correction.
- As long as the correctness of data is disputed the data shall be blocked for processing.
- Disclosing Personal Data to a third party, such as a Third-Party Sub-Processor, shall only be allowed with prior written consent from and only for the purposes identified in Principle Agreements or SOW or Purchase order with RPS. RPS shall have the right to evaluate the contractual terms and conditions.

Prior to Vendor transferring Personal Data to a Third-Party Sub-Processor, the Vendor shall ensure responsibilities of Vendor and of the Third-Party Sub-Processor are clearly described and implemented as part of the commercial contract.

ANNEX III

LIST OF APPROVED SUB-PROCESSORS

In the provision of services, the use of sub-processors will be strictly limited to those necessary for the performance of your services as agreed. The utilization of any sub-processor for purposes beyond this scope will require prior approval from RPS.

EXHIBIT B: EU PROCESSOR-TO-PROCESSOR STANDARD CONTRCTUAL CLAUSES

Section I

Clause 1

Purpose and scope

(e)   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.

(f)   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').

(g)   These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(h)   The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(c)   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.

(d)   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

(c)   Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

    (i)   Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

    (ii)   Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

    (iii)   Clause 9(a), (c), (d) and (e);

    (iv)   Clause 12(a), (d) and (f);

    (v)   Clause 13;

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

    (vii)   Clause 16(e); and

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

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

Clause 4

Interpretation

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

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

(f)   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

Module III: 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.

8.1 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.

8.2 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.

8.3 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.

8.4 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).

8.5 Security of processing

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

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without

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

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

8.6   Sensitive data

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

8.7   Onward transfers

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

(i)   the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii)   the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii)   the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv)   the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.8   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

(f)   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 prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

(g)   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.

(h)   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.

(i)   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.

(j)   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

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

(e)   The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(f)   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

(g)   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.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body 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.

(h)   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.

(i)   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:

    (iii)   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;

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

(j)   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.

(k)   The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(l)   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

(h)   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.

(i)   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.

(j)   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.

(k)   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.

(l)   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.

(m)   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.

(n)   The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(c)   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.

(d)   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

(g)   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.

(h)   The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(iv)   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;

    (v)   the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

    (vi)   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.

(i)   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.

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

(k)   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). The data exporter shall forward the notification to the controller.

(l)   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, 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 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

15.3   Notification

(f)   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:

    (iii)   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

(iv)   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.

The data exporter shall forward the notification to the controller.

(g)   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.

(h)   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.). The data exporter shall forward the information to the controller.

(i)   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.

(j)   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.

15.4   Review of legality and data minimisation

(d)   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).

(e)   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. The data exporter shall make the assessment available to the controller.

(f)   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

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

(g)   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).

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

   (iv)   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;

   (v)   the data importer is in substantial or persistent breach of these Clauses; or

   (vi)   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 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.

(i)   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.

(j)   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

This document was updated on October 1, 2024

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 Ireland.

Clause 18

Choice of forum and jurisdiction

(e)   Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(f)   The Parties agree that those shall be the courts of (specify Member State).

(g)   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.

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

ANNEX I

B. LIST OF PARTIES

Data exporter(s):

Name: RPS Consulting Ltd and its Affiliates

Address: As per Agreement/Statement of Work/ Purchase Order

Activities relevant to the data transferred under these Clauses: A*greement/Statement of Work/ Purchase Order*

Role: Controller/Processor

Data importer(s): [*As per Agreement/Statement of Work/ Purchase Order*]

Name: ……………………….

Address: ……………………….

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

Role: Controller/Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose Personal Data is transferred	Individuals of whom Personal Data is Processed by or on behalf of the Data Exporter
Categories of Personal Data transferred	Categories of Personal Data (including sensitive Personal Data) transferred would be data, that, in connection with the performance of Processing services under the Agreement/Statement of Work/ Purchase Order
Restrictions or safeguards for personal data including sensitive data :	Safeguards implemented to tranfer Personal Data are as stated in Annex II- Technical and Organizational Measures
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	As necessary for Data Importers provision of Processing servicing and performance of its obligations under the Agreement/Statement of Work/ Purchase Order
Nature of the Processing	The nature of the Processing activity will be that as necessary for Data Importer's provision of the Processing activities and performance of its obligations under these Agreement/Statement of Work/ Purchase Order.
Purpose(s) of the data transfer and further Processing	Data Importer will Process European Personal Data in accordance with the terms of the Agreement/Statement of Work/ Purchase Order, for the purpose of performing the services under the Agreement/Statement of Work/ Purchase Order.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period	For the duration of the Agreement/Statement of Work/ Purchase Order pursuant to which the Data Importer will provide its Services to RPS, and thereafter as necessary to comply with applicable laws or contractual obligations.
For transfers to (sub-) processors, specify subject matter, nature and duration of the processing	As stated in Annex III

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13	The supervisory authority identified by the data exporter or as required by any local law.

<div align="center">

ANNEX II

</div>

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

Vendor shall implement measures designed to:

- deny unauthorized persons access to data-processing equipment used for processing Personal Data(equipment access control);
- prevent the unauthorized reading, copying, modification or removal of data media (data media control);
- prevent the unauthorized input of Personal Data and the unauthorized inspection, modification ordeletion of stored Personal Data (storage control);
- prevent the use of automated data-processing systems by unauthorized persons using data communication equipment (user control);
- ensure that persons authorized to use an automated data-processing system only have access to thePersonal Data covered by their access authorization (data access control);
- ensure that it is possible to verify and establish to which individuals Personal Data have been or may be transmitted or made available using data communication equipment (communication control);
- ensure that it is subsequently possible to verify and establish which Personal Data have been put intoautomated data-processing systems and when and by whom the input was made (input control);
- prevent the unauthorized reading, copying, modification or deletion of Personal Data during transfers ofthose data or during transportation of data media (transport control);
- ensure that installed systems may, in case of interruption, be restored (recovery);
- ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored Personal Data cannot be corrupted by means of a malfunctioning of the system (integrity).

Vendor shall comply with the below mentioned Information Security Measures

- Set direction for and show commitment to information security. At a minimum there shall be a high-level information security policy and supporting program that applies enterprise-wide.
- Information shall not be excessively stored, printed, copied, disclosed or Processed by other meansoutside the purpose for use.
- Information shall be processed and stored logically separated from the Vendors own information and from that of other customers.
- Upon conclusion or termination of Vendor's work for RPS, the Vendor shall sanitize and securely destroy (or at RPS's election return to RPS) all copies of all Information, including all backup and archival copies, in any electronic or non-electronic form.
- Access to Information shall be restricted to Personnel individually and on a need to know basis.

<div align="center">

This document was updated on October 1, 2024

</div>

- Access to information needs to be on individual basis and at least password protected, and computerscreens need to be locked in case of absence.
- Storage media containing Personal or Information shall be encrypted during transport and destroyedin a secure way.
- Records shall be kept in an auditable manner showing which Information has been has beenaccessed, modified, disclosed or disposed.
- Cryptographic controls shall be used in compliance with all relevant agreements, legislation andregulations.
- Physical access to Vendor buildings shall be restricted to Personnel individually and on a need to have basis.
- Systems containing Information shall be protected by firewall(s) and properly hardened, i.e. removing or disabling software and functionalities that are not being used.
- Vendor networks used to access Information or networks shall have security controls that can protect against unauthorized traffic interception or interference by making use of firewalls, intrusiondetection/prevention, etc.
- Wireless network connections transferring Information shall be encrypted according to bestpractice.
- Vendor shall deploy technology to scan Vendor's corporate email for viruses and malicious code
  and links and keep such technology up to date.
- Disclosing Information to a third party, such as a Third-Party Sub-Processor, shall only be allowed with prior written consent from and only for the purposes identified in contractual agreements withRPS.
- Third Party Sub-Processors shall be restricted to only the necessary access, use, retention and disclosure of Information needed to fulfil contractual obligations.
- Third Party Sub-Processors shall be given clear instructions on security measures for protecting Information.
- Vendor shall have a documented security incident management process to detect and handle incidents. Vendor shall report confirmed security incidents or weaknesses involving Information or Services for as soon as practicable or as otherwise agreed upon.
- Security related incidents should be reported to: <nimesh.aggarwal@rpsconsulting.in> , appointed point of contact or as otherwise specified in contractual agreements.
- Vendor shall cooperate fully with in dealing with these reports. Cooperation may include providingaccess to computer-based evidence data for forensic evaluation.

Vendor shall comply with the below mentioned Data Privacy Measures

- Set direction for and show commitment to privacy. At a minimum there shall be a high-level privacy policy that applies enterprise-wide and assignment of overall responsibility for privacy to a top-level executive or equivalent.
- Vendor shall ensure protection and privacy of Personal Data related to Services in accordance with relevant data protection legislation and regulations.
- Personal Data, including redacted or Anonymized Personal Data, shall not be used for any other purposethan meeting Principle agreements or SOW or Purchase order with RPS.
- Personal Data collected for different purposes shall be processed separately.
- Personal Data shall not be accessed without prior authorization.
- Authorized Personnel shall only have access to the least amount of Personal Data to carry out their job duty.

This document was updated on October 1, 2024

- Personnel with access to Personal Data shall be required to take appropriate data privacy training on a regular basis.
- Personal Data shall be retained for only as long as necessary to fulfill the stated purposes in Principle Agreements or SOW or Purchase order with RPS, or as required by law or regulations, and shall thereafter be appropriately returned or disposed at the choice of RPS.
- The disposal of Personal Data shall be recorded to certify to that such disposal has taken place.
- Where the return or disposal of some, or all of the Personal Data is prevented by law or regulation, the Personal Data shall be kept confidential or anonymized and shall no longer be processed shall be informed if such obligations exist immediately when Vendor becomes aware of them.
- Personal Data shall not be excessively stored, printed, copied, disclosed or other means of Processing outside the purpose for use.
- The Data Subject shall be provided with access to his or her Personal Data for review.
- In the event the Data Subject does not have direct access to his or her Personal Data, the Personal Data shall be transferred to in order to support any Data Subject request, without answering the request unless authorized to do so.
- Inaccurate Personal Data shall be corrected when the Data Subject or on the Data Subject's behalf, has
  made a request for correction.
- As long as the correctness of data is disputed the data shall be blocked for processing.
- Disclosing Personal Data to a third party, such as a Third-Party Sub-Processor, shall only be allowed with prior written consent from and only for the purposes identified in Principle Agreements or SOW or Purchase order with RPS. RPS shall have the right to evaluate the contractual terms and conditions.

Prior to Vendor transferring Personal Data to a Third-Party Sub-Processor, the Vendor shall ensure responsibilities of Vendor and of the Third-Party Sub-Processor are clearly described and implemented as part of the commercial contract.

ANNEX III

LIST OF APPROVED SUB-PROCESSORS

In the provision of services, the use of sub-processors will be strictly limited to those necessary for the performance of your services as agreed. The utilization of any sub-processor for purposes beyond this scope will require prior approval from RPS.

This document was updated on October 1, 2024

EXHIBIT C: EU PROCESSOR-TO-CONTROLLER STANDARD CONTRCTUAL CLAUSES

Section I

Clause 1

Purpose and scope

(i)   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.

(j)   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').

(k)   These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(l)   The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(e)   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.

(f)   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

(e)   Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

  (i)   Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

  (ii)   Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

  (iii)   Clause 9(a), (c), (d) and (e);

  (iv)   Clause 12(a), (d) and (f);

  (v)   Clause 13;

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

  (vii)

  (viii) Clause 16(e); and

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

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

Clause 4

Interpretation

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

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

(i)   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

Module IV: Transfer Processor to Controller

8.1. Instructions

(a)   The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b)   The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c)   The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d)   After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of Processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (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 of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality

8.3   Documentation and Compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.
(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

(k)   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 prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

(l)   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.

(m)   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.

(n)   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.

(o)   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

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

(h)   The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(i)   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

(m)   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.

   The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body 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.

(n)   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.

(o)   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:

   (v)   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;

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

(p)   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.

(q)   The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(r)   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

(o)   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.

(p)   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.

(q)   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.

(r)   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.

(s)   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.

(t)   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.

(u)   The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(e)   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.

(f)   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

(m)   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.

(n)   The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(vii)   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;

(viii)   the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(ix)   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.

(o)   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.

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

(q)   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). The data exporter shall forward the notification to the controller.

(r)   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, 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 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

15.5   Notification

(k)   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:

(v)   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

(vi)   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.

The data exporter shall forward the notification to the controller.

(l)   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.

(m)   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.). The data exporter shall forward the information to the controller.

(n)   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.

(o)   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.

15.6   Review of legality and data minimisation

(g)   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).

(h)   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. The data exporter shall make the assessment available to the controller.

(i)   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

This document was updated on October 1, 2024

Non-compliance with the Clauses and termination

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

(l)   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).

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

(vii)   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;

(viii)   the data importer is in substantial or persistent breach of these Clauses; or

(ix)   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 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.

(n)   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.

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

Clause *17*

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(i)   Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(j)   The Parties agree that those shall be the courts of (specify Member State).

(k)   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.

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [As per Agreement/Statement of Work/ Purchase Order]

Name: ………………………….

Address: …………………………

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

Role: Controller/Processor

Data importer(s):

Name: RPS Consulting Ltd and its affiliates

Address: As per Agreement/Statement of Work/ Purchase Order

Activities relevant to the data transferred under these Clauses: Agreement/Statement of Work/ Purchase Order

Role: Controller/Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose Personal Data is transferred	Individuals of whom Personal Data is Processed by or on behalf of the Data Exporter
Categories of Personal Data transferred	Categories of Personal Data (including sensitive Personal Data) transferred would be data, that, in connection with the performance of Processing services under the Agreement/Statement of Work/ Purchase Order
Restrictions or safeguards for personal data including sensitive data :	Safeguards implemented to tranfer Personal Data are as stated in Annex II- Technical and Organizational Measures
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	As necessary for Data Importers provision of Processing servicing and performance of its obligations under the Agreement/Statement of Work/ Purchase Order
Nature of the Processing	The nature of the Processing activity will be that as necessary for Data Importer's provision of the Processing activities and performance of its obligations under these Agreement/Statement of Work/ Purchase Order.
Purpose(s) of the data transfer and further Processing	Data Importer will Process European Personal Data in accordance with the terms of the Agreement/Statement of Work/ Purchase Order, for the purpose of performing the services under the Agreement/Statement of Work/ Purchase Order.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period	For the duration of the Agreement/Statement of Work/ Purchase Order pursuant to which the Data Importer will provide its Services to RPS, and thereafter as necessary to comply with applicable laws or contractual obligations.
For transfers to (sub-) processors, specify subject matter, nature and duration of the processing	As stated in Annex III

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13	The supervisory authority identified by the data exporter or as required by any local law.

This document was updated on October 1, 2024

ANNEX II

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

The technical and organizational measures must be described in specific (and not generic) terms. Description of the technical and organizational measures implemented by the Non-EU/EEA Vendors (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Examples of possible measures which needs to be taken by Non-EU/EEA Vendors

-Measures of pseudonymization and encryption of personal data.

-Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.

-Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

-Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing.

-Measures for user identification and authorization.

-Measures for the protection of data during transmission.

-Measures for the protection of data during storage.

-Measures for ensuring physical security of locations at which personal data are processed.

-Measures for ensuring events logging.

-Measures for ensuring system configuration, including default configuration.

-Measures for internal IT and IT security governance and management.

-Measures for certification/assurance of processes and products.

-Measures for ensuring data minimization.

-Measures for ensuring data quality.

-Measures for ensuring limited data retention.

-Measures for ensuring accountability.

-Measures for allowing data portability and ensuring erasure.

APPENDIX-II

TECHNICAL AND ORGANISATIONAL MEASURES FOR NON-EU/EEA VENDORS

Vendor shall implement measures designed to:

- deny unauthorized persons access to data-processing equipment used for processing Personal Data(equipment access control);
- prevent the unauthorized reading, copying, modification or removal of data media (data media control);
- prevent the unauthorized input of Personal Data and the unauthorized inspection, modification ordeletion of stored Personal Data (storage control);
- prevent the use of automated data-processing systems by unauthorized persons using data communication equipment (user control);
- ensure that persons authorized to use an automated data-processing system only have access to thePersonal Data covered by their access authorization (data access control);
- ensure that it is possible to verify and establish to which individuals Personal Data have been or may be transmitted or made available using data communication equipment (communication control);
- ensure that it is subsequently possible to verify and establish which Personal Data have been put intoautomated data-processing systems and when and by whom the input was made (input control);
- prevent the unauthorized reading, copying, modification or deletion of Personal Data during transfers ofthose data or during transportation of data media (transport control);
- ensure that installed systems may, in case of interruption, be restored (recovery);
- ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored Personal Data cannot be corrupted by means of a malfunctioning of the system (integrity).

Vendor shall comply with the below mentioned Information Security Measures

- Set direction for and show commitment to information security. At a minimum there shall be a high-level information security policy and supporting program that applies enterprise-wide.
- Information shall not be excessively stored, printed, copied, disclosed or Processed by other meansoutside the purpose for use.
- Information shall be processed and stored logically separated from the Vendors own information and from that of other customers.
- Upon conclusion or termination of Vendor's work for RPS, the Vendor shall sanitize and securely destroy (or at RPS's election return to RPS) all copies of all Information, including all backup and archival copies, in any electronic or non-electronic form.
- Access to Information shall be restricted to Personnel individually and on a need to know basis.
- Access to information needs to be on individual basis and at least password protected, and computerscreens need to be locked in case of absence.
- Storage media containing Personal or Information shall be encrypted during transport and destroyedin a secure way.
- Records shall be kept in an auditable manner showing which Information has

been has beenaccessed, modified, disclosed or disposed.

- Cryptographic controls shall be used in compliance with all relevant agreements, legislation andregulations.
- Physical access to Vendor buildings shall be restricted to Personnel individually and on a need to have basis.
- Systems containing Information shall be protected by firewall(s) and properly hardened, i.e. removing or disabling software and functionalities that are not being used.
- Vendor networks used to access Information or networks shall have security controls that can protect against unauthorized traffic interception or interference by making use of firewalls, intrusiondetection/prevention, etc.
- Wireless network connections transferring Information shall be encrypted according to bestpractice.
- Vendor shall deploy technology to scan Vendor's corporate email for viruses and malicious code
  and links and keep such technology up to date.
- Disclosing Information to a third party, such as a Third-Party Sub-Processor, shall only be allowed with prior written consent from and only for the purposes identified in contractual agreements with RPS.
- Third Party Sub-Processors shall be restricted to only the necessary access, use, retention and disclosure of Information needed to fulfil contractual obligations.
- Third Party Sub-Processors shall be given clear instructions on security measures for protecting Information.
- Vendor shall have a documented security incident management process to detect and handle incidents. Vendor shall report confirmed security incidents or weaknesses involving Information or Services for as soon as practicable or as otherwise agreed upon.
- Security related incidents should be reported to: <nimesh.aggarwal@rpsconsulting.in>, appointed point of contact or as otherwise specified in contractual agreements.

- Vendor shall cooperate fully with in dealing with these reports. Cooperation may include providingaccess to computer-based evidence data for forensic evaluation.

Vendor shall comply with the below mentioned Data Privacy Measures

- Set direction for and show commitment to privacy. At a minimum there shall be a high-level privacy policy that applies enterprise-wide and assignment of overall responsibility for privacy to a top-level executive or equivalent.
- Vendor shall ensure protection and privacy of Personal Data related to Services in accordance with relevant data protection legislation and regulations.
- Personal Data, including redacted or Anonymized Personal Data, shall not be used for any other purposethan meeting Principle agreements or SOW or Purchase order with RPS.
- Personal Data collected for different purposes shall be processed separately.
- Personal Data shall not be accessed without prior authorization.
- Authorized Personnel shall only have access to the least amount of Personal Data to carry out their job duty.
- Personnel with access to Personal Data shall be required to take appropriate data privacy training on a regular basis.
- Personal Data shall be retained for only as long as necessary to fulfill the stated purposes in Principle Agreements or SOW or Purchase order with RPS, or as required by law or regulations, and shall thereafter be appropriately returned or disposed at the choice of RPS.

- The disposal of Personal Data shall be recorded to certify to that such disposal has taken place.
- Where the return or disposal of some, or all of the Personal Data is prevented by law or regulation, the Personal Data shall be kept confidential or anonymized and shall no longer be processed shall be informed if such obligations exist immediately when Vendor becomes aware of them.
- Personal Data shall not be excessively stored, printed, copied, disclosed or other means of Processing outside the purpose for use.
- The Data Subject shall be provided with access to his or her Personal Data for review.
- In the event the Data Subject does not have direct access to his or her Personal Data, the Personal Data shall be transferred to in order to support any Data Subject request, without answering the request unless authorized to do so.
- Inaccurate Personal Data shall be corrected when the Data Subject or on the Data Subject's behalf, has

  made a request for correction.
- As long as the correctness of data is disputed the data shall be blocked for processing.
- Disclosing Personal Data to a third party, such as a Third-Party Sub-Processor, shall only be allowed with prior written consent from and only for the purposes identified in Principle Agreements or SOW or Purchase order with RPS. RPS shall have the right to evaluate the contractual terms and conditions.
- Prior to Vendor transferring Personal Data to a Third-Party Sub-Processor, the Vendor shall ensure responsibilities of Vendor and of the Third-Party Sub-Processor are clearly described and implemented as part of the commercial contract.

APPENDIX-IV

UNITED KINGDOM (U.K.) STANDARD CONTRACTUAL CLAUSES

This APPENDIX-IV is part of the U.K. Addendum and must be read with EU Standard Contractual Clauses where required.

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

Part 1: Tables

Table 1: Parties

Start date	Effective as of the DTA Effective Date.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Same as listed in Annex I.A of Appendix -I,II, III of the Approved EU SCCs.	Same as listed in Annex I.A of Appendix -I,II, III of the Approved EU SCCs.
Key Contact	Same as listed in Annex I.A of Appendix -I,II, III of the Approved EU SCCs.	Same as listed in Annex I.A of Appendix -I,II, III of the Approved EU SCCs.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐The version of the Approved EU SCCs which this Addendum is appended to, including the either Appendix I, II or III Information.

Table 3: Appendix Information

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

This document was updated on October 1, 2024

Annex 1A: List of Parties: same as Annex 1 of either Appendix I or II to the EU Approved EU SCCs

Annex 1B: Description of Transfer: same as Annex 1 of either Appendix I or II to the EU Approved EU SCCs

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: same as Annex 2 of either Appendix I or II to the EU Approved EU SCCs

Annex III: List of Sub processors: same as Annex III of either Appendix I or II to the EU Approved EU SCCs.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1 and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.

Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in either Appendix I or II.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 17.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

This document was updated on October 1, 2024

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 9 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum override the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 10 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 14 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b.   In Clause 2, delete the words:

"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";

c.   Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d.   Clause 8.8(i) is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

e.   References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article(s) or Section(s) of UK Data Protection Laws;

f.   References to Regulation (EU) 2018/1725 are removed;

g.   References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

h.   Clause 13(a) is not used;

i.   The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

j.   In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

k.   Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

l.   Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer

before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

m. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 17, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the Addendum; and/or

    b. its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

This document was updated on October 1, 2024