Data Processing Addendum

This Data Processing Addendum and its Attachment 1, Attachment 2,Attachment 3,Attachment 4, (together the "**DPA**") form part of the Jile Terms of Service available at https://www.jile.io/terms ("Principal Agreement") between: (i) You (the "**Controller**" or "**Customer**") and (ii) Tata Consultancy Services Limited ("**Processor**" or "**TCS**") and is executed by and between the Customer and TCS, individually referred to as a "**Party**" and jointly referred to as "**Parties**".

Recitals:

A. Whereas this DPA sets out the terms and conditions under which TCS will process the Customer's Personal Data for the purpose of the Principal Agreement.

B. Whereas, Parties agree that Customer is the Controller and TCS is the Processor of the Personal Data as defined in the Data Protection Laws.

1. Definitions

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

(a) "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is under common control or ownership with either Customer or TCS (as the context allows), 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;

(b) "**Controller to Processor SCCs**" means (a) in relation to the EU, the standard contractual clauses which establish a level of adequate protection for personal data and approved by the EU Commission or (b) in relation to the UK, relevant standard data protection clauses specified in either regulations pursuant to Article 46(2)(c) UK GDPR; or a document issued (and not withdrawn) pursuant to Article 46(2)(d) UK GDPR, as the same are revised or updated from time to time by the European Commission and the UK and incorporated in this DPA in the Attachment 2.

(c) "**Data Protection Laws**" 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 (also named "General Data Protection Regulation" or "EU **GDPR**"), and the EU GDPR as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"), together with applicable legislation implementing or supplementing the same or otherwise relating to the Processing of Personal Data of natural persons, together with binding guidance and codes of practice issued from time to time by relevant supervisory authorities, including, but not limited to the California Consumer Privacy act of 2018, as amended by the California Privacy Rights Act of 2020 ("CCPA"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, and the Connecticut Data Privacy Act, and also the Specific Privacy Laws as included in Attachment 4, together with any amending or replacement legislation and any regulations issued thereunder;

(d) "GDPR" means the EU GDPR and/or the UK GDPR as the context requires;

(e) "**Personal Data**" means any Personal Data Processed by TCS or any TCS Affiliate (i) on behalf of Customer or any Customer Affiliate; or (ii) on behalf of any client of Customer or any Customer Affiliate, or (iii) otherwise Processed by TCS or TCS Affiliate, in each case pursuant to or in connection with instructions given by Customer consistent with the Principal Agreement;

(f) "**Services**" means the services to be supplied by TCS and/or TCS Affiliates to Customer and/or Customer Affiliates pursuant to the Principal Agreement.

(g) **"Specific Privacy Laws"**. To the extent the processing of Customer Personal Data is subject to an applicable Data Privacy Law described in Attachment 4 (Specific Privacy Laws), the corresponding terms in Attachment 4 will apply in addition to these general terms herein and prevail as described in Section 11.2 .

1.2 The terms "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Process**", "**Processor**" and "**Supervisory Authority**" have the same meanings as described in the Data Protection Laws and cognate terms shall be construed accordingly.

2. Processing

2.1 This DPA applies to all Processing of Personal Data performed by TCS on behalf of the Controller within the scope of the Principal Agreement.

2.2 TCS shall process Personal Data on behalf of the Controller. Such Processing shall include all activities detailed in the DPA. Within the scope of this DPA, the Controller shall be solely responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Personal Data to TCS and the lawfulness of having Personal Data Processed on behalf of the Controller.

2.3 TCS shall Process Personal Data only on documented instructions from the Controller. The Controller's individual instructions shall, initially, be those detailed in this DPA. The Controller shall, subsequently, be entitled to, in writing or in in text form, modifying, amending or replacing such individual instructions by issuing such instructions to the point of contact designated by Processor. Instructions that are not part of the scope of Services under the Principle Agreement shall be treated as requests for changes to such agreement. The Controller shall, without undue delay, confirm in writing or in text form any instruction issued orally.

2.4 Attachment 1 to the DPA (or a form substantially similar to Attachment 1) defines the subject matter and duration of the Processing, the nature and purpose of the Processing, the categories of data subjects, types of Personal Data, special categories of Personal Data that will be processed under the Principal Agreement as well as the Processing activities implemented under the Principal Agreement.

2.5 The Controller shall:

(a) determine the purposes and means of the Processing of Personal Data;

(b) act in compliance with Data Protection Laws; and

(c) not instruct TCS to Process Personal Data in a manner that would constitute a breach of Data Protection Laws.

2.6 TCS shall:

(a) Process Personal Data only on behalf of the Controller in accordance with the Controller's documented instructions set forth in this DPA (unless required by law to act otherwise, wherein TCS shall communicate such alternative instructions to the Controller unless prohibited by law), or as otherwise necessary to perform its obligations under the Data Protection Laws and/or Specific Privacy Law.

(b) take reasonable steps to ensure the reliability of persons authorised to process the Personal Data and ensure that persons Processing the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) be entitled to make its own day to day operational decisions and the same shall not be deemed to breach of the instructions of the Controller.

3. Certifications and Audits

3.1 Upon Customer's request, and provided that the Parties have a Non-Disclosure Agreement in place applicable, if necessary, also to information provided by any of the sub-processors, TCS will make available the following documents and information to Customer:

(a) the certificate issued in relation to the ISO 27001 certification (or other documentation evidencing compliance with other standards substantially equivalent to ISO 27001).

3.2 In relation to such certification, TCS will conduct periodic audits of the system involved in the processing of Personal Data on behalf of Customer. Such audits conducted by qualified, independent third-party auditors will result in the generation of an audit report ("Audit Report"), which will be TCS' Confidential Information.

3.3 Upon Customer's request, and provided that the Parties have a Non-Disclosure Agreement in place applicable, if necessary, also to information provided by any of the sub-processors, TCS will make available to Customer a copy of the last Audit Report so that Customer can verify TCS' compliance with its obligations under this DPA.

3.4 To the extent Customer's audit requirements under the Standard Contractual Clauses cannot reasonably be satisfied through audit reports, documentation or compliance information as defined in articles from 3.1 to 3.3, TCS will promptly respond to Customer's additional audit instructions. Before the commencement of an audit, Customer and TCS will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit TCS to unreasonably delay performance of the audit. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to TCS, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any data from TCS' other customers or to TCS' systems or facilities not involved in the scope Principal Agreement. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time TCS expends for any such audit, in addition to the rates for services performed by TCS.

4. Personal Data Breaches

4.1 Processor shall notify Customer without undue delay after becoming aware of a Personal Data Breach. Such notice shall:

(a) describe the nature of the Personal Data Breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the Personal Data Breach; and

(d) describe the measures taken or to be taken by Processor to address the Personal Data Breach, including, where appropriate, the measures to mitigate the possible adverse effects.

4.2 Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases.

5. Sub-processing

5.1 TCS is generally authorized by the Controller to engage with sub-processors and Processor Affiliates, subject to the condition that TCS (i) publishes any intended changes to its use of sub-processors on the webpage https://www.jile.io/security.html and (ii) includes terms in its contract with each sub-processor which are no less protective than those set out in this DPA. In addition, Parties agree that the Controller has pre-approved all sub-processors listed at https://www.jile.io/security.html or as listed in Attachment 2 - Annexure III.

5.2 TCS is generally authorized to transfer any Personal Data to a country outside the EU/EEA to other TCS Affiliate as sub-processor and to the third party service providers listed at https://www.jile.io/security.html.

5.2.1 Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, and/or where Personal Data of a UK based Controller is processed in a country outside the UK and any

country, organization or territory acknowledged by the UK as safe country with an adequate level of data protection under Art. 45 UK GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:

(a) TCS and Customer enter into the Controller to Processor SCCs;

(b) Where required by the Data Protection Laws, Customer enters into the Controller to Processor SCCs with each relevant Subprocessor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by TCS or and the Subprocessor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Subprocessor (represented by TCS) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"); and/or

(c) Other Controllers whose use of the Software or Services has been authorized by Customer under the Principal Agreement may also enter into Standard Contractual Clauses with TCS and/or the relevant Subprocessors in the same manner as Customer in accordance with Sections 5.2(a) and (b) above. In such case, Customer will enter into the Standard Contractual Clauses on behalf of the other Controllers.

6. Return or deletion of Personal Data

6.1 As soon as it is no longer required for the performance of TCS's obligations under the Principal Agreement, and at the latest upon termination or expiration of the Principal Agreement, Processor will delete all Personal Data 30 days from such date, unless (i) before the expiry of the aforementioned 30 days, the Controller elects to have all copies of the Personal Data returned to it (subject to the Controller bearing Processor' reasonable costs); or (ii) any law to which TCS or any TCS Affiliate is subject requires the retention of the Personal Data (in which case the Personal Data shall only be retained for as long as is necessary to comply with that requirement).

7. Security

7.1 The technical and organizational measures applied by TCS as of the DPA Effective Date are set forth on the webpage https://www.jile.io/security.html and as introduced as Attachment 2 – Annex II. The Controller is familiar with these technical and organizational measures, and the Controller has confirmed that such measures ensure a level of security appropriate to the risk.

7.2 TCS reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.

7.3 The Controller and TCS shall fulfil their obligations under Article 32.1 (d) GDPR to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

8. Data subject requests

8.1 To the extent permitted by law, Processor will inform Customer of requests from data subjects exercising their data subject rights (access, rectification, erasure, restriction, data portability and objection) addressed directly to Processor. TCS may not directly reply to such requests unless expressly instructed to do so by the Controller unless otherwise required by law. Customer shall be responsible to respond to such requests of data subjects assisted by Processor, insofar as possible.

8.2 TCS shall assist Customer or the relevant Customer Affiliate by appropriate technical and organizational measures taking into account the information available to Processor and nature of Processing, insofar as this is possible, for the fulfilment of Customer's or the relevant Customer Affiliate's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

9. Assistance

9.1 Taking into account the information available to Processor and nature of Processing, Processor will assist Customer by technical and organizational measures in ensuring compliance with Customer's obligations relating to the security of Processing, the notification of Personal Data breach and the data protection impact assessment.

9.2 At the request of Controller, TCS shall assist the Controller in (i) allowing data subjects to exercise their rights under the GDPR, (ii) in meeting the Controller's GDPR obligations in relation to the security of Processing, the notification of Personal Data breach and data protection impact assessments. All assistance performed by Processor under the DPA shall be subject to a charge agreed in writing by the Parties.

10. Liability

10.1 Notwithstanding anything to the contrary in the Principal Agreement, the Parties agree that their liability in the performance of their obligations under this Data Processing Addendum and all documents entered into pursuant to it shall be subject to the limitation of liability agreed in section 14 of the Principal Agreement. For the avoidance of doubt, this section does not replace or waive the rights and obligations of each party in accordance with Article 82 GDPR.

11. Miscellaneous

11.1 The Parties agree that, except as modified herein, the terms of the Principal Agreement shall remain in full force and effect. Notwithstanding anything to the contrary in the Principal Agreement, in the event of inconsistencies between the provisions of this DPA and the provisions of the Principal Agreement, the provisions of this DPA shall prevail.

11.2 In case of any conflict, the data protection regulations of this DPA shall take precedence over the regulations of the Principle Agreement where this is necessary to give full force and effect to the GDPR or any other Data Protection law applicable to the Processing of Personal Data. Further, in case of any conflict between the data protection regulations of this DPA and Specific Privacy Laws, in case applicable, the regulations of the Specific Privacy Law shall prevail. Where individual regulations of this DPA are invalid or unenforceable, the validity and enforceability of the other regulations of this DPA shall not be affected.

11.3 This DPA comes into force on the same date as the Principal Agreement. Except where this DPA stipulates obligations beyond the term of the Principle Agreement, the term of this DPA shall be the term of the Principal Agreement.

Attachment 1 to the DPA – Details of Processing activities

This form includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR, which the Processor carries out on behalf of the Controller in accordance with the DPA.

1. **Subject matter and duration of the Processing of Customer Personal Data**

The subject matter and duration of the Processing of the Personal Data are set out in the Principal Agreement.

2. Nature and purpose of the Processing of the Personal Data

The purpose of the Processing of the Personal Data is set out in the Principal Agreement and this DPA, and include the following Processing activities:

1. *Provisioning of the SaaS Services, Software or Services as used or requested by the Customer or its Authorized Users*
2. *To provide support service including troubleshooting and repairing problems or issues or incidents*
3. *Periodic maintenance of the Software or Services Environment, include installaling latest updates or patches*
4. *Delivering any professional services, including but not limited to, planning, advice, guidance, data migration, deployment, training and solution/software development services.*
5. *Business operations as part of delivery of Services includes customer account management for billing and administrative purpose, activating Subscription Plan, internal reporting for business forecasting, revenue etc. and proactive logs monitoring for combatting fraud, cybercrime, or cyber-attacks that may affect the Services.*

3. Data subjects

The Personal Data transferred concern the following categories of data subjects:

employees, contractors, business partners or other individuals having Personal Data stored in the cloud Service.

4. Categories of data

The Personal Data transferred concern the following categories of data:

Customer determines the categories of data. The transferred Personal Data typically relates to the following categories of data: *name, phone numbers, e-mail address, time zone, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data that Authorized User enter into the Software.*

Special categories of data (if appropriate)

No sensitive Personal Data is Processed under the Principal Agreement

5. Processing operations

The Personal Data transferred will be subject to the following basic Processing activities:

- *provisioning of the Software's Services;*
- *communication to Authorized Users;*
- *storage of Personal Data;*
- *upload any fixes or upgrades to the Software;*
- *back up of Personal Data;*
- *computer processing of Personal Data, including data transmission, data retrieval, data access;*
- *network access to allow Personal Datatransfer;*
- *execution of instructions of Customer in accordance with the Agreement.*

Attachment 2 to the DPA – Controller to Processor SCCs

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

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

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

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

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

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

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(b), 8.9(a), (c), (d) and (e);

(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);

(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 OR **[Not used]]**

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

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 ([2]) (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

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

(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.

(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 ([5]);

(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).

(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. 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 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.

(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.).

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

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

15.2 Review of legality and data minimization

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

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

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority 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

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

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 the Netherlands.

(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.

Footnotes:

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these

Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(2) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(3) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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

(5) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

ANNEX I

A. **LIST OF PARTIES**

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

1.	Name: [Customer entity name as *per relevant order.*] Address: [Customer address as *per relevant order*] Contact person's name, position and contact details: [Customer authorized person placing the relevant order] Activities relevant to the data transferred under these Clauses: [as per attachment 1 of DPA] Signature and date: [Customer authorized person placing the relevant order] Role (controller/processor): Controller
2.	[.....]

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

1.	Name: [*Tata Consultancy Services Ltd*] Address: [TCS House, Raveline Street, 21 D S Marg, Fort, Mumbai 400001, India] Contact person's name, position and contact details: [Ashvini Saxena....CEG Unit Head] Activities relevant to the data transferred under these Clauses: [*as per attachment 1 of DPA.*] Signature and date: [30-Aug-2024] Role (controller/processor): Processor
2.	[.....]

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

[refer to Attachment 1 to the DPA - Details of Processing activities]

Categories of personal data transferred

[refer to Attachment 1 to the DPA - Details of Processing activities]

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

[Continuous]

Nature of the processing

[refer to Attachment 1 to the DPA - Details of Processing activities.]

Purpose(s) of the data transfer and further processing

[refer to Attachment 1 to the DPA - Details of Processing activities.]

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

[*Data will be deleted 30 days after the end date of the Subscription Term mentioned in the relevant Order form if it is not renewed.*]

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

[https://www.jile.io/security.html]

C. **COMPETENT SUPERVISORY AUTHORITY**

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

[Supervisory Authority of the EU Member Country in which the Customer / Exporter is organized.]

[*INSERT PAGE BREAK HERE*]

ANNEX II

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

Measures	**Description**
Measures of pseudonymization and encryption of personal data	PII Data is encrypted using AES 256 encryption
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	All PII Data is encrypted and stored. The data is backed up at regular intervals to avoid the loss of data and data integrity is maintained every time when the data is change.
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	All the business data is backed up and the backup are maintained in a different geographic location from the application hosting location. In case of any incident the backup is available for restoring and continuing the business
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	The application goes through TCS internal IP Safe certification process for Product quality. ARM process is being initiated every three months for Application Deployment. Audit is conducted every six months for the Operations. This ensures that every process and controls are validated continuously.
Measures for user identification and authorization	Application provides default in built authentication and authorization model. Along with it the Application has ability to connect with the SAML IDP for Authentication
Measures for the protection of data during transmission	All data sent from the Server to Customers has been encrypted using SSL certificate with SHA-256 encryption key and TSL 1.2 Protocol. This ensures the data is protected during the transmission
Measures for the protection of data during storage	Data storage disks are encrypted using Azure Disk encryption. Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant.
Measures for ensuring physical security of locations at which personal data are processed	The Application is deployed in three different geographic regions in Azure Cloud Server - US, UK and India. The details of the physical security is detailed here https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security#physical-security
Measures for ensuring events logging	All System and Application events are logged. The logs are connected with SIEM system for analysis and reporting.
Measures for ensuring system configuration, including default configuration	Application default configuration is documented and reviewed every three months as a part of ARM Process
Measures for internal IT and IT security governance and management	We are certified for ISO 27001. The product undergoes security certification for Product Development, Deployment and Operational activities
Measures for certification/assurance of processes and products	The Product goes through IP Safe certification for every Release and ARM process is followed for all the Product Deployments
Measures for ensuring data minimization	Only relevant PII data is collected and will be used only for the purpose for which it was collected
Measures for ensuring data quality	All PII Data collected is validated for quality and there is no requirement of merging with other sources. The data quality is kept intact throughout the lifecycle
Measures for ensuring limited data retention	All business data is retained in the system till the subscription is active. The data will be removed from the system post 30 days after subscription expiry
Measures for ensuring accountability	Any additional fields for PII data collection will undergo a Data Privacy review process and the PII data will be made available only based on purpose of usage

Measures for allowing data portability and ensuring erasure	All business data can be fetched from the system using Application APIs in the standard json format. The data will be removed from the system post 30 days after subscription expiry

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

[*INSERT PAGE BREAK HERE*]

ANNEX III

LIST OF SUB-PROCESSORS

Information relating to sub-processors is available at the following link:

https://www.jile.io/security.

EXPLANATORY NOTE:

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

The controller has authorized the use of the following sub-processors details of which are available at: https://www.jile.io/security.htm

Attachment 3 UK INTERNATIONAL DATA TRANSFER ADDENDUM

Table 1: Parties

Start date	[As per term of the Principle Agreement]

The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Role	**CONTROLLER**	**PROCESSOR**
Parties' details	Full legal name:	Full legal name:
	[Customer entity name a*s per relevant order.*]	Tata Consultancy Services Limited
	Trading name (if different):	Trading name (if different):
	Main address (if a company registered address):	Main address (if a company registered address):
	[Customer address a*s per relevant order*]	Nirmal Building, 9th Floor, Nariman Point, Mumbai 400 021, India with its UK branch office at 18 Grosvenor Place, London SW1X 7HS
	Official registration number (if any) (company number or similar identifier):	Official registration number (if any) (company number or similar identifier):
	Registered in England and Wales with registration number [ ]	11-84781
Key contacts	[Customer authorized person placing the relevant order]	[TCS authorized person]
Signature (if required for the purposes of Section 2)	Signature of the Exporter set out at end of this agreement.	Signature of the Importer set out at end of this agreement.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs to which this Addendum is attached, including the Appendix Information: Date: Date of the last signature of the Data Transfer Agreement

Table 3: Appendix Information

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

Annex 1A: List of Parties: As set out in the Approved EU SCCs to which this Addendum in attached.
Annex 1B: Description of Transfer: As set out in the Approved EU SCCs to which this Addendum in attached.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set out in the Approved EU SCCs to which this Addendum in attached.
Annex III: List of Sub processors: As set out in the Approved EU SCCs to which this Addendum in attached.

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 1A 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 Table 2, including the Appendix Information.

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 28 January 2022, as it is revised under Section 18.

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.

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 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides 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 11 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 15 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 8.7(i) of Module 1 is replaced with:

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

    e. Clause 8.8(i) of Modules 2 and 3 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;"

    f. 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 or Section of UK Data Protection Laws;

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

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

    i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

    j. Clause 13(a) and Part C of Annex I are not used;

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

    l. 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;";

m. Clause 17 is replaced with:

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

n. 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

o. 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 18, 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

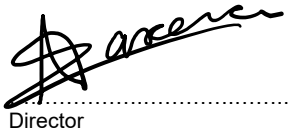
b its risk under the Addendum,

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 agreement has been entered into on the date of the last signature below.

Signed by [Customer authorized person placing the relevant order]	Authorized Signatory Digital Signature ……

for and on behalf of **[Customer entity name a*s per relevant order.*]**	Director Date: [ ]
Signed by [Ashvini Saxena CEG Unit Head] for and on behalf of **Tata Consultancy Services Ltd**	Authorized Signatory Digital Signature  ..... Director Date: [30-Aug-2024]

Attachment 4 to the DPA – Specific Privacy Laws

Latin America Addendum

This Addendum is entered into by the Customer identified on the Principal Agreement ("Customer") and Tata Consultancy Services Limited or its Affiliate identified on the Principal Agreement ("Processor" or "TCS"). With respect to TCS`s processing of Personal Data of individuals in **Argentina, Brazil, Chile, Colombia, Ecuador, Guatemala, Mexico, Peru and/or Uruguay**; as applicable, the below terms will apply in addition to the other terms and conditions outlined in this DPA and the Principal Agreement.

1. Definitions

1.1. **"Latam Data Protection Laws"** means (a) Brazilian General Data Protection Law (LGPD); (b) Argentina, Act no. 25.326 of Protection of Personal Data; (c) Colombia, Statutory Law 1581 of 2012 and Decree 1377 of 2013; (d) Chile, Law 19,628/1999 'On the protection of private life; (e) Ecuador, Personal Data Protection Organic Law; (f) Mexico, The Federal Law on the Protection of Personal Data held by Private Parties; (g) Peru, The Personal Data Protection Law N° 29733 (PDPL); (h) Uruguay, Data Protection Act Law No. 18.331, Decree No. 414/009 and Decree 64/2020; (i) all applicable laws, regulations or requirements or regulatory guidance, in any jurisdiction, related to data protection, privacy or confidentiality of Personal Data, in each case of the foregoing as applicable to the Processing of Personal Data under this DPA.

1.2. The terms "Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Processor", "Process/Processing" (and "Processed") and "Supervisory Authority", among others that are applicable to this DPA, shall have the meaning provided to those terms or similar terms under the Latam Data Protection Laws in the context of their applicability under this DPA (e.g., Personal Data has the meaning provided under Data Protection Act Law No. 18.331, so the definition of "Personal Data" is expanded to include any kind of information related to a legal entity identified or identifiable).

2. General

2.1. The Parties shall comply with all applicable Latam Data Protection Laws in the Processing of Personal Data.

3. International Data Transfers.

3.1. Any transfer of Personal Data to a third country, which does not provide for an adequate level of data protection in accordance with Latam Data Protection Laws ("Restricted Transfer") requires the execution of Data Transfer Agreements between the data exporter and the data importer. "Data Transfer Agreement" means any contractual instrument recognized under applicable Latam Data Protection Laws, such as the Ibero-American Data Protection Network ('RIPD') model contractual clauses ('MCCs') for the international transfer of personal data, which establish a level of adequate protection for the international transfer of personal data.

3.2. **Argentine Transfers.** In the event of a Restricted Transfer to a recipient outside of Argentina, then such transfers shall be governed by the MCCs for the international transfer of personal data between controller and processor, issued by the RIPD and approved by the AAIP through Resolution 198/2023 ("Argentine SCCs"), which shall be entered into and incorporated into this DPA by reference and:

3.2.1. Clause 7: Option 1 (general written authorization) is selected.

3.2.2. The data exporter is the Customer of the Principal Agreement.

3.2.3. The data importer is TCS as specified in the DPA for the provision of the services defined in the Principal Agreement.

3.2.4. The Customer's address is the address on the Principal Agreement.

3.2.5. TCS' address is the address on the Principal Agreement.

3.2.6. Attachment 1 of this DPA provide details of the Restricted Transfer and the processing activities.

3.2.7. The full text of the Argentine SCCs is available here: https://www.boletinoficial.gob.ar/detalleAviso/primera/296189/20231018

3.3. **Brazilian Transfers.** In accordance with LGPD, the below terms will apply to international data transfers:

3.3.1. The parties shall:

3.3.1.1. maintain a record of the processing activity of data transfer (Article 37 of the LGPD);

3.3.1.2. adopt security, technical, and administrative measures capable of protecting personal data from unauthorised access and situations of destruction, loss, communication, or any type of harmful or illicit processing activities (Article 46 of the LGPD);

3.3.1.3. ensure the security of the information even after the end of the processing activity (Article 47 of the LGPD); and

3.3.1.4. comply with the principles of the LGPD (Article 6 of the LGPD).

3.3.1.5. The Controller shall:

3.3.1.6. to provide and disclose the privacy notice to the data subjects;

3.3.1.7. to indicate the legal basis for the processing activity of data transfers (Articles. 7, 11, and 14 of the LGPD);

3.3.1.8. to draft the Data Protection Impact Assessment (Articles 5 XVII and 38 of the LGPD);

3.3.1.9. to guarantee the collection of the freely given, informed, and unambiguous (Articles 5 (XVII), 7º(I), 8 (§2º), and 11(I) of the LGPD);

3.3.1.10. to inform the data subject in case the consent was collected as the legal basis and if there is a change in the purpose, form, and duration of treatment, identification of the Controller, and information about the sharing of information (Article 8 (§6) of the LGPD);

3.3.1.11. to facilitate access for data subjects to the information on data processing, including the identification of the Controller, their contact details, and information on the shared use of data by the Controller (Article 9 (III)(IV) and (V) of the LGPD);

3.3.1.12. if the legitimate interest is the legal basis, the Controller must guarantee the use is strictly necessary (Article 10 (§1) of the LGPD) and adopt the appropriate measures of transparency (Article 10 (§ 2) of the LGPD) and the balance between its interest and the rights and freedoms of the data subject;

3.3.1.13. to abstain to disclose or share sensitive personal data related to health, with the purpose of obtaining economic advantage, except in cases related to the provision of health services, pharmaceutical assistance, and health care in order to allow data portability when requested by the holder, or the financial and administrative transactions resulting from the use and provision of the services mentioned (Article 11 (§4) of the LGPD), as informed on Section 6;

3.3.1.14. to ensure the exercise of the data subject's rights and respond to their requests (Article 18 (caput) (§§3 and 4) of LGPD); and

3.3.1.15. communicate to the ANPD and the data subject whenever there is a data breach that represents high risk to the data subjects. (Article 48 of the LGPD).

3.3.2. The Processor shall:

3.3.2.1. process the Personal Data according to the instructions provided by the Controller (Article 39 of the LGPD); and

3.3.2.2. collaborate with the Controller to meet its obligations, in accordance with the principle of good faith (Article 6 of the LGPD).

3.4. **Peruvian Transfers.** In the event of a Restricted Transfer to a recipient outside of Peru, then such transfers shall be governed by the MCCs for the international transfer of personal data between controller and processor, issued by the RIPD and approved by the National Authority for the Protection of Personal Data by its Directorial Resolution No. 0074-2022-JUS/DGTAIPD ("Peruvian SCCs"). The Peruvian SCCs shall be entered into and incorporated into this DPA by reference and:

3.4.1. Clause 7: Option 1 (general written authorization) is selected.

3.4.2. The data exporter is the Customer of the Principal Agreement.

3.4.3. The data importer is TCS as specified in the DPA for the provision of the services defined in the Principal Agreement.

3.4.4. The Customer's address is the address on the Principal Agreement.

3.4.5. TCS' address is the address on the Principal Agreement.

3.4.6. Attachment 1 of this DPA provide details of the Restricted Transfer and the processing activities.

3.4.7. The full text of the Peruvian SCCs is available here: https://www.gob.pe/institucion/minjus/normas-legales/3617286-0074-2022-jus-dgtaipd

3.5. **Colombian Transfers.** The transmission of Personal Data to the Processor located outside of Colombia will be applicable under the following terms and conditions:

3.5.1. The Controller is in Colombia and the Processor is located outside of Colombia.

3.5.2. The Controller will send by written their Personal Data processing policies so the Processor shall comply with those policies.

3.5.3. The Processor will process the Personal Data only for, for the benefit of, and in the name of the Controller;

3.5.4. Attachment 1 of this DPA provide details of description of the processing and processing activities to be performed by Processor;

3.5.5. The Processor will process the personal data within the purposes established by the Controller; and

3.5.6. The Processor will ensure the confidentiality, security, and integrity of the Personal Data.

3.6. **Uruguayan Transfers.**

3.6.1. The Customer is the Controller and is located in Uruguay.

3.6.2. TCS and TCS Affiliates will be the Processor.

3.6.3. The Customer agrees and consents to transfer Personal Data to TCS and TCS Affiliates, even if they are located in non-adequate countries according to Resolution 23/2021 issued by the Supervisory Authority, having the relevant consents, as applicable.

3.6.4. The Processor will be compliant with the levels of protection and security of personal data defined in the DPA so that the collection and processing of data comply with the requirements of the regulation on the protection of personal data in force in Uruguay and other regulations - national and international - of the matter.

Asia Pacific Provisions Addendum

This Addendum is entered into by the Customer ("Customer") identified on the Principal Agreement and Tata Consultancy Services Limited ("TCS"). With respect to TCS`s processing of Personal Data of data subjects residing in the Asia Pacific region, the bellow terms will apply in addition to the other terms and conditions outlined in the TCS privacy notice, the Principal Agreement and the DPA. Capitalized terms not otherwise defined in the DPA will have the meanings given to them under the applicable Data Privacy Law as specified below.

AUSTRALIA

1. When Personal Information of Australians customers is being processed, Parties shall comply with the terms and provisions of the Privacy Act 1988 (“Privacy Act”).

2. For the purposes of this Addendum, Parties agree that TCS is the Processor, who shall process the Personal Information on behalf of Customer and/or under Customer`s instructions, and Customer is the Controller, who owns and decides the process that Personal Information would be submitted to.

3. The Customer warrants that the Personal Information has been collected in accordance with Privacy Act and if required by TCS, shall provide the evidence that the data subject was notified in accordance with Privacy Act. If required, and Customer fails to provide the evidence that Personal Information was collected in compliance with Privacy Act, TCS shall be entitled to immediately interrupt its services without incurring in penalties and/or breach of contract obligations.

4. Customer warrants that it has implemented the security measures defined by Privacy Act and is the only responsible for communicating the Office of the Australian Information Commissioner (“OIAC”) and all affected data subjects if a Personal Information breach occurs without undue delay. Customer may request TCS`s support to develop the notice, and TCS shall implement its best endeavors to support Customer, however, the context, the moment to notice the breach and eventually costs arising from it shall be bear by Customer.

CHINA

1. When Personal Information of residents of Mainland China (excluding residents of Hong Kong, Macau and Taiwan) are being processed, Parties shall comply with the terms and provisions of the PRC Cybersecurity Law (CSL”), the PRC Data Security Law (“DSL”), the PRC Personal Information Protection Law (“PIPL”) and all data protection or privacy laws, regulations, regulatory requirements, guidelines, and codes of practice applicable to the performance of the Principal Agreement (“Data Privacy Laws”).

2. For the purposes of this Addendum, TCS is the Entrusted Processing Party, who shall process the Personal Information on behalf of Customer and/or under Customer`s instructions, and Customer is the Personal Information Handler who makes its own decision on the purpose, the means of processing and other matters relating to the Personal Information processing.

3. Whether Customer intends to transfer its Personal Information to an overseas entity, it may be required by Data Privacy Laws to pass a security assessment, obtain certification from professional institutions or entering a Standard Contract with such entity. Customer is solely responsible to comply with such Data Privacy Laws requirements. If required, TCS may support Customer to comply with Data Privacy Laws requirement, however, any costs arising from it shall be bear by Customer.

4. The Customer warrants that the Personal Information has been collected in accordance with Data Privacy Laws and if required by TCS, shall provide the respective legal basis in which Personal Information has been processed. If Customer fails to provide the legal base, TCS shall be entitled to immediately interrupt its services without incurring in penalties and/or breach of contract obligations.

5. Customer warrants that it has implemented the security measures defined by Data Privacy Laws and is the only responsible for communicating the Personal Information Protection Authorities and affected data subjects if a Personal Information breach occurs without undue delay. Customer may request TCS`s support to develop the notice, an TCS shall implement its best endeavors to support Customer, however, the context, the moment to notice the breach and eventually costs arising from it shall be bear by Customer.

HONG KONG

1. When Personal Data of residents of Special Administrative Region of Hong Kong are being processed, Parties shall comply with the terms and provisions of the Personal Data (Privacy) Ordinance (Chapter 486 of Laws of Hong Kong) (“PDPO”).

2. For the purposes of this Addendum, TCS is the Data Processor who processes Personal Data on behalf of Customer and/or under Customer`s instructions and Customer is the Data User who, either alone or jointly with other persons, controls the collection, holding, processing or use of Personal Data.

3. Customer warrants that have collected the Personal Data for the purposes informed to data subjects and will not instruct TCS to process the Personal Data for other purposes, except if data subject has provided its consent to do so.

4. The Customer warrants that the Personal Data has been collected in accordance with PDPO and if required by TCS, shall provide the evidence that the data subject was notified in accordance with PDPO. If required and Customer fails to provide the evidence that Personal Data was collected in compliance with PDPO and/or data subject has consented the processing for another purpose

as mentioned in section 3 above, TCS shall be entitled to immediately interrupt its services without incurring in penalties and/or breach of contract obligations.

INDONESIA

1. When Personal Data of Indonesian customers are being processed, Parties shall comply with the terms and provisions of the Law n. 27 Year 2022 on Personal Data Protection ("PDP Law").

2. For the purposes of this Addendum, Parties agree that TCS is the Processor, who shall process the Personal Data on behalf of Customer and/or under Customer`s instructions, and Customer is the Controller, who owns and decide the process that Personal Data would be submitted.

3. The Customer warrants that the Personal Data has been collected in accordance with PDP Law and if required by TCS, shall provide the respective legal basis in which Personal Data has been processed. If required and Customer fails to provide the legal base, TCS shall be entitled to immediately interrupt its services without incurring in penalties and/or breach of contract obligations.

4. Customer warrants that it has implemented the security measures defined by PDP Law and is the only responsible for communicating the data protection authority and all affected data subjects if a Personal Data breach occurs, no later than 3 (three) days from the event. Customer may request TCS`s support to develop the notice, and TCS shall implement its best endeavors to support Customer, however, the context, the moment to notice the breach and eventually costs arising from it shall be bear by Customer.

MALAYSIA

1. When Personal Data of Malaysian customers are being processed, Parties shall comply with the terms and provisions of the Personal Data Protection Act 2010 ("PDPA").

2. For the purposes of this Addendum, Parties agree that TCS is the Processor, who shall process the Personal Data on behalf of Customer and/or under Customer`s instructions, and Customer is the Data User, who owns and decide the process that Personal Data would be submitted.

3. The Customer warrants that the Personal Data has been collected in accordance with PDPA and if required by TCS, shall provide the respective legal basis in which Personal Data has been processed. If required and Customer fails to provide the legal base, TCS shall be entitled to immediately interrupt its services without incurring in penalties and/or breach of contract obligations.

4. Customer warrants that it is registered and authorized by Personal Data Protection Department ("PDP") to collect and process the Personal Data as a Data User.

5. Customer warrants that it has implemented the security measures defined by PDPA and is the only responsible for communicating the PDP and all affected data subjects if a Personal Data breach occurs, no later than 72 (seventy-two) hours of becoming aware of the Personal Data breach incident. Customer may request TCS`s support to develop the notice, and TCS shall implement its endeavors to support Customer, however, the context, the moment to notice the breach and eventually costs arising from it shall be bear by Customer.

NEW ZEALAND

1. When Personal Information of New Zealand citizens are being processed, Parties shall comply with the terms and provisions of the Privacy Act 2020 ("Privacy Act").

2. For the purposes of this Addendum, Parties agree that TCS is the Processor, who shall process the Personal Information on behalf of Customer and/or under Customer`s instructions, and Customer is the Controller, who owns and decide the process that Personal Information would be submitted.

3. The Customer warrants that the Personal Information has been collected in accordance with Privacy Act and if required by TCS, shall provide the evidence that the data subject was notified in accordance with Privacy Act. If required and, Customer fails to provide the evidence that Personal Information was collected in compliance with Privacy Act, TCS shall be entitled to immediately interrupt its services without incurring in penalties and/or breach of contract obligations.

4. Customer warrants that it has implemented the security measures defined by Privacy Act and is the only responsible for communicating the New Zealand Privacy Commissioner and all affected data subjects if a Personal Information breach occurs without undue delay. Customer may request TCS`s support to develop the notice, and TCS shall implement its best endeavors to support Customer, however, the context, the moment to notice the breach and eventually costs arising from it shall be bear by Customer.

PHILIPPINES

1. When Personal Data of residents of Republic of The Philippines are being processed, Parties shall comply with the terms and provisions of the Data Privacy Act ("DPA").

2. For the purposes of this Addendum, TCS is the Company who shall process the Personal Data on behalf of Customer and/or under Customer`s instructions, and Customer is the Personal Information Controller who makes its own decision on the purpose, the means of processing and other matters relating to the Personal Data.

3. The Customer warrants that the Personal Data has been collected in accordance with DPA and if required by TCS, shall provide the respective legal basis in which Personal Data has been processed. If required and Customer fails to provide the legal base, TCS shall be entitled to immediately interrupt its services without incurring in penalties and/or breach of contract obligations.

4. Customer warrants that its Data Protection Officer (DPO) is duly registered and approved by The Philippine National Privacy Commission ("NPC") and shall provide DPO contact details to its users/customers/employees and, if required, to TCS.

5. Customer warrants that it has implemented the security measures defined by DPA and is the only responsible for communicating the NPC and affected data subjects if a Personal Data breach occurs within 72 (seventy-two) hours of having knowledge of such event. Customer may request TCS`s support to develop the notice, a TCS shall implement its best endeavors to support Customer, however, the context, the moment to notice the breach and eventually costs arising from it shall be bear by Customer.

SINGAPORE

1. When Personal Data of residents of Singapore are being processed, Parties shall comply with the terms and provisions of the Personal Data Protection Act ("PDPA").

2. For the purposes of this Addendum, TCS is the Data Intermediary who shall process the Personal Data on behalf of Customer and/or under Customer`s instructions, and Customer is the Organization who makes its own decision on the purpose, the means of processing and other matters relating to the Personal Data.

3. The Customer warrants that the Personal Data has been collected in accordance with PDPA and if required by TCS, shall provide the respective legal basis in which Personal Data has been processed. If required and Customer fails to provide the legal base, TCS shall be entitled to immediately interrupt its services without incurring in penalties and/or breach of contract obligations.

4. Customer warrants that it has implemented the security measures defined by PDPA and is the only responsible for communicating the Personal Data Protection Commission ("PDPO") and all affected data subjects no later than 3 (three) calendar days from the day that the Customer determines that a data breach is a notifiable data breach. Customer may request TCS`s support to develop the notice, and TCS shall implement its best endeavors to support Customer, however, the context, the moment to notice the breach and eventually costs arising from it shall be bear by Customer.

SOUTH KOREA

1. When Personal Information of residents of South Korea are being processed, Parties shall comply with the terms and provisions of the Personal Information Protection Act ("PIPA") and its implementing regulations.

2. For the purposes of this Addendum, TCS is the Processor, who shall process the Personal Information on behalf of Customer and/or under Customer`s instructions, and Customer is the Personal Information Controller who makes its own decision on the purpose, the means of processing and other matters relating to the Personal Information.

3. The Customer warrants that the Personal Information has been collected in accordance with PIPA and if required by TCS, shall provide the respective legal basis in which Personal Information has been processed. If required and Customer fails to provide the legal base, TCS shall be entitled to immediately interrupt its services without incurring in penalties and/or breach of contract obligations.

4. Customer warrants that it has implemented the security measures defined by PIPA and is the only responsible for communicating the Personal Information Protection Commission ("PIPC") and all affected data subjects if a Personal Information breach occurs without undue delay. Customer may request TCS`s support to develop the notice, and TCS shall implement its best endeavors to support Customer, however, the context, the moment to notice the breach and eventually costs arising from it shall be bear by Customer.

TAIWAN

1. When Personal Data of residents of Taiwan are being processed, Parties shall comply with the terms and provisions of the Personal Data Protection Act ("PDPA") and the Enforcement Rules of the Personal Data Protection Act ("the Enforcement Rules").

2. For the purposes of this Addendum, Parties agree that TCS is the Processor, who shall process the Personal Data on behalf of Customer and/or under Customer`s instructions, and Customer is the Controller, who owns and decide the process that Personal Data would be submitted.

3. The Customer warrants that the Personal Data has been collected in accordance with PDPA and the Enforcement Rules and if required by TCS, shall provide evidence that the data subject was notified in accordance with PDPA and the Enforcement Rules. If required and Customer fails to provide the evidence that Personal Data was collected in compliance with PDPA and the Enforcement Rules, TCS shall be entitled to immediately interrupt its services without incurring in penalties and/or breach of contract obligations.

4. Customer warrants that it has implemented the security measures defined by PDPA and the Enforcement Rules and is the only responsible for communicating the Data Protection Authorities and all affected data subjects if a Personal Data breach occurs without undue delay. Customer may request TCS`s support to develop the notice, and TCS shall implement its best endeavors to support Customer, however, the context, the moment to notice the breach and eventually costs arising from it shall be bear by Customer.

THAILAND

1. When Personal Data of residents of the Kingdom of Thailand are being processed, Parties shall comply with the terms and provisions of the Thailand`s Personal Data Protection Act B.E. 2562 (2019) ("PDPA").

2. For the purposes of this Addendum, Parties agree that TCS is the Processor, who shall process the Personal Data on behalf of Customer and/or under Customer`s instructions, and Customer is the Controller, who owns and decide the process that Personal Data would be submitted.

3. The Customer warrants that the Personal Data has been collected in accordance with PDPA and if required by TCS, shall provide the respective legal basis in which Personal Data has been processed. If required and Customer fails to provide the legal base, TCS shall be entitled to immediately interrupt its services without incurring in penalties and/or breach of contract obligations.

4. Customer warrants that it has implemented the security measures defined by PDPA and is the only responsible for communicating the Office of the Personal Data Protection Committee and all affected data subjects without undue delay and, where feasible, within 72 (seventy-two) hours after having become aware of the breach. Customer may request TCS`s support to develop the notice, and TCS shall implement its endeavors to support Customer, however, the context, the moment to notice the breach and eventually costs arising from it shall be bear by Customer.

CCPA Addendum

1. Capitalized terms used and not defined herein have the meaning(s) given to them in the Principal Agreement. In the event of any conflict between this CCPA Addendum and the Principal Agreement, the terms of this CCPA Addendum prevail.

2. The terms "Business Purpose", "Contractor", "Personal Information", "Sensitive Personal Information", "Sale", "Share", and "Service Provider" have the meanings ascribed to them in the CCPA. In this CCPA Addendum, the term Personal Information includes Sensitive Personal Information.

3. TCS is a Service Provider in performing the Services under the Principal Agreement. TCS will not:

    a. Sell or Share any Personal Information;

b. Retain, use or disclose any Personal Information (i) for any purpose other than for the Business Purposes specified in the Principal Agreement, including for any commercial purpose, or (ii) outside of the direct business relationship between TCS and the Customer; or

c. Combine Personal Information received from or on behalf of the Customer with Personal Information received from or on behalf of any third party, or collected from TCS' own interaction with individuals or data subjects, except to perform the following Business Purposes that are permitted by the CCPA and the Principal Agreement:

   i. Helping to ensure security and integrity to the extent the use of the Personal Information is reasonably necessary and proportionate for these purposes;

   ii. Debugging to identify and repair errors that impair existing functionality;

   iii. Performing services on behalf of the Customer, including customer account management for billing and administrative purposes, activating subscription plans, data migration, deployment, training and solution/software development services;

   iv. Undertaking internal research for technological development; and

   v. Undertaking activities to maintain the quality of a service that is controlled by the business and to improve, upgrade, or enhance such service.

4. The parties acknowledge that the Personal Information the Customer discloses to TCS is provided only for the limited and specified purposes set forth in the Principal Agreement. TCS shall provide the same level of protection to Personal Information as is required by the CCPA and as is more fully set out in the Principal Agreement.

5. The Customer may take such reasonable steps as may be necessary to (i) remediate TCS's unauthorized use of Personal Information, and (ii) to ensure that Personal Information is used in accordance with the terms of this CCPA Addendum and the Principal Agreement.

6. TCS will promptly notify the Customer if it makes a determination that it can no longer meet the requirements under this CCPA Addendum.