SCHEDULE D

DATA PROCESSING ADDENDUM

1. In addition to the defined terms set out in the Agreement, the following words and expressions shall have the following meanings when used in this Schedule D:

Controller	means the Client;
Data Subject	means the natural person whose Personal Data is made available by the Controller to the Processor;
DPA	means this Data Processing Addendum;
Personal Data	means any information about the Data Subject provided by the Controller to the Processor in accordance with the Agreement, which is considered personal data under the Regulation;
Processor	means CTO2B;
Purpose of Data Processing	means the execution of the Agreement and the fulfillment of the respective Party's rights and obligations under that Agreement;
Regulation	means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
Sub-processor	means a third party authorised under this DPA to have logical access to and process Personal Data in order to provide parts of the services and related technical support;
Standard Contractual Clauses	means any processor engaged by the Processor or its Affiliates to assist in the performance of Processor's obligations in relation to the performance under the Agreement.

2. The definitions used in the DPA which are not defined in Clause 1.1 hereabove have the same meaning as in the Regulation and the Agreement.

3. PROCESSING OF PERSONAL DATA

3.1. The Parties acknowledge and agree that the Controller and its Affiliates shall act as data controllers and the Processor and its Affiliates act as a data processors in the processing of the Personal Data, except in the following cases (i) where the Controller acts as a processor of the Personal Data, in which case the Processor acts as a Sub-Processor; or (ii) as otherwise provided in this DPA.

3.2. All Personal Data categories and Data Subject categories which the Controller may provide to the Processor under this DPA are listed in the Personal Data categories and Data Subject categories lists set out in Annex 1 to the DPA. The Controller shall be responsible for drawing up and updating these lists.

4. PROCESSOR'S OBLIGATIONS

4.1. The Processor shall process the Personal Data only for the Purpose of Data Processing and in accordance with the requirements of the Regulation, the Agreement, the provisions of this DPA, and the instructions of the Controller. The provisions of this DPA and the Agreement, as well as any service configuration made from time to time by the Controller using the tools provided by the services, shall be deemed to be the only documented instructions of the Controller with respect to the processing of Personal Data. Any other instructions from the Controller must be agreed in advance in writing between the Parties and may be subject to additional terms and conditions.

4.2. Upon receipt of a request from a Data Subject, including but not limited to a request for information, access, rectification, erasure, or restriction of processing, the Processor shall forward such request, together with all relevant information, to the Controller without undue delay and no later than 2 working days from the date of receipt.

4.3. The Processor shall cooperate with the Controller in order to ensure compliance with the obligations set out in Articles 32 – 36 of the Regulation.

4.4. The Processor shall, upon a request from the Controller, immediately cease any processing of Personal Data other than storage and shall not resume such processing until instructed to do so by the Controller. If such an instruction hinders or prevents the Processor from properly performing its duties under the Agreement, the Processor shall be entitled to (i) suspend all or part of its obligations under the Agreement until the Parties agree on the resumption of the Personal Data processing operations, or (ii) unilaterally terminate the Agreement without recourse to court by notifying the Controller within 7 days.

5. CONTROLLER'S OBLIGATIONS

5.1. The Controller shall process Personal Data in compliance with the Regulation, including any applicable requirements to notify Data Subjects of the Processor's role as a processor and to obtain their consent for such processing.

5.2. The Controller determines, at its discretion, the categories of Personal Data and Data Subjects to be provided to the Processor and shall ensure that the Processor has the right to process the Personal Data for the Purposes of Data Processing under this DPA.

6. SECURITY AND TECHNICAL AND ORGANIZATIONAL MEASURES

6.1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of varying probability and severity for the rights and freedoms of natural persons, the Processor undertakes, within the limits of its responsibility, to implement the appropriate technical and organizational measures necessary to ensure the security as required by Article 32 of Regulation and the protection and proper implementation of the rights of the Data Subjects as established in the Regulation. In selecting and implementing the appropriate technical and organizational measures, the Processor shall in particular take into account the risks arising from the processing of the Personal Data of the Data Subjects due to unintentional or unlawful deletion, loss, alteration or unauthorized disclosure or unauthorized access to the Personal Data stored or otherwise processed.

6.2. The Processor shall select and establish the technical and organizational measures necessary to achieve the objective set forth in Clause 6.1 of the DPA and to provide adequate security, but in any case, such measures shall be without prejudice to the requirements of the Regulation. The list of such technical and organizational measures is attached to this DPA as Annex 2.

6.3. The Controller has the right to make recommendations to the Processor regarding the application of technical and organizational measures. The Processor shall take such recommendations into account, evaluate them and (i) provide the Controller with a reasoned refusal to carry out the Controller's instructions or (ii) implement the recommended measures without undue delay.

6.4. Notwithstanding the provisions of Clauses 6.1 and 6.2, where either Party entrusts the other Party with means of remote access to the information systems, the Controller shall, at its own expense, ensure the maximum security of the connection required for such connection and shall apply the necessary and appropriate tools and measures for the protection of data, traffic and communications (e.g. encryption, etc.).

7. AUDIT RIGHTS

7.1. Upon request, the Processor shall provide the Controller with the necessary information to demonstrate the implementation of technical and organizational measures, including copies of its most recent third party audits or certifications. If the Controller reasonably believes that such documentation is insufficient to confirm compliance with this DPA, the Controller may, after consultation with the Processor and with the Processor's consent (which shall not be unreasonably withheld or delayed), audit the Processor's compliance. This audit may be carried out by the Controller or a mutually agreed accredited third party auditor who is not a competitor of the Processor, during normal business hours, without disruption to operations, upon reasonable prior written notice and subject to confidentiality agreements. Audits shall not be conducted more than once per calendar year unless required by a competent regulatory authority.

7.2. The Controller shall be responsible for all costs associated with such audits, including reasonable costs of the Processor's time and resources, in addition to the service fees under the individual agreement. Prior to the commencement of any audit, the Controller and the Processor shall mutually agree on the scope, timing and duration of the audit, which shall be limited to matters specific to the Controller.

7.3. Unless prohibited by applicable law, the Controller shall provide the Processor with copies of any audit reports prepared under this Section. The Controller may use such reports only to comply with regulatory audit requirements or to confirm compliance with this DPA. The Controller shall promptly notify the Processor of any non-compliance discovered during the audit.

8. SUB-PROCESSORS

8.1. The Controller hereby grants the Processor general prior consent to engage Sub-Processors to process the Personal Data on behalf of the Processor within the scope and for the purposes set out in this DPA.

8.2. The Processor shall engage only those Sub-Processors who ensure the following: (i) the implementation of appropriate technical and organizational measures; (ii) the processing of the Personal Data in accordance with the requirements of the Regulation; and (iii) the protection of the rights of the Data Subject.

8.3. The Processor shall ensure that a written agreement has been concluded with any sub-processors it uses, under which the sub-processors undertake to comply with the responsibilities of the data processor set out in this DPA, at least to the extent that they apply to the Processor. The Processor shall be liable to the Controller for the fulfilment of the obligations of the Sub-Processors engaged.

8.4. The list of engaged Sub-Processors will be made available on the Processor’s website. The Processor shall notify the Controller of its intention to replace or engage a new Sub-Processor by updating this information on the Processor's website in advance of the planned event. If the Controller continues to use the Processor’s services after the replacement or engagement of a new Sub-Processor and after the notification referred to in clause 8.4 of this DPA, the Controller shall be deemed to have accepted such actions by the Processor.

8.5. In the event that the Controller (i) does not authorize the Processor to use a Sub-Processor or to change one Sub-Processor with another or (ii) revokes the given general consent to use Sub-Processor to perform all or part of the Personal Data processing activities, the Processor is entitled, at its discretion, to (a) suspend the performance of all or part of its obligations under the Agreement until the Parties agree on the use or change of the Sub-Processor; or (b) unilaterally and without recourse to the court to terminate the Agreement by notifying the Controller within 7 days.

9. DATA TRANSFERS OUTSIDE THE EEA

9.1. The Processor shall process Personal Data solely within the territories of the member states of the European Economic Area.

9.2. If the Processor intends to process Personal Data outside the territories of the member states of the European Economic Area (EEA), it shall, prior to such processing, notify the Controller by updating this information on the Processor’s website, and the Controller shall, without undue delay and with consent that is not unreasonably withheld, authorize such transfer if, in the sole discretion of the Processor, it is necessary for the performance of the Agreement or this DPA, including transfers to jurisdictions for which the European Commission has not issued an adequacy decision, provided that the Processor has implemented a transfer solution compliant with the Regulation. This may include:

9.2.1. *Standard Contractual Clauses*: For transfers of the Personal Data covered by the Regulation, the Processor will process data in accordance with the Standard Contractual Clauses. The Parties agree that for the purposes of the descriptions in the Standard Contractual Clauses, the Processor acts as the “*data importer*” and the Controller as the “*data exporter*,” regardless of the Controller’s location or role. If the Controller is a controller, the Controller-to-Processor Clauses (Module 2) will apply; if the Controller is a processor, the Processor-to-Processor Clauses (Module 3) will apply;

9.2.2. *Alternative Safeguards*: Other safeguards under Article 46 of the Regulation;

9.2.3. *Derogations*: Applicable derogations under Article 49 of the Regulation.

9.3. If the Processor becomes unable to comply with the obligations in this Section, it shall immediately notify the Controller and take reasonable steps to cease processing outside the EEA. The Personal Data originating in the EEA will then only be processed within EEA unless the Processor obtains prior written consent or complies with the level of protection required under this Section.

10. **CONFIDENTIALITY**

10.1. The Processor shall ensure the confidentiality of the Personal Data and shall not disclose it to third parties except in the cases and procedures specified in the Agreement or in the DPA or in the Regulation, nor shall it use the Personal Data for its own purposes or for the purposes of third parties, except for the Purpose of Data Processing.

10.2. The Processor has the right to grant access to the Personal Data only to authorised persons (employees, consultants, etc.) who need such access in order to perform the Agreement and who undertake to process the Personal Data in accordance with the conditions set out in this DPA and to maintain confidentiality both during the performance of the Agreement and after its expiry to the same extent as the Processor itself.

11. PERSONAL DATA BREACHES

11.1. In the event of a Personal Data Breach or if the Processor reasonably suspects such a breach, the Processor shall immediately, but in any case, not later than within 60 hours after learning about it, inform the Controller in writing and provide the information and data available on such a breach. The Personal Data Breach notification must contain:

11.1.1. a description of the nature of the Personal Data Breach that has occurred or is likely to occur, including, if possible, the categories and approximate numbers of the data subjects concerned, as well as the relevant categories of Personal Data and approximate figures;

11.1.2. the name of the data protection officer or other contact person who can provide more information (the name of the legal entity) and the contact details;

11.1.3. a description of the measures taken or proposed by the Processor to eliminate the Personal Data Breach, including measures to reduce potential negative consequences.

11.2. At the request of the Controller, the Processor shall, taking into account the technical possibilities, provide the Controller without undue delay with any other necessary documents, information and data, which are necessary for the Controller to establish and/or verify the fact of the Personal Data Breach, to investigate its circumstances and to take immediate measures to eliminate the Breach or to mitigate its possible negative consequences.

12. LIABILITY

12.1. The Controller shall hold harmless, indemnify and defend the Processor and its Affiliates, trustees, directors, officers, employees, and agents and the successor and assigns of any of the foregoing (collectively, the “Indemnitees”) from and against any and all liabilities, damages, penalties, expenses and/or losses, including reasonable attorneys’ fees and other expenses of litigation resulting from any claims, actions, suits, or proceedings brought by third parties (any of the foregoing, a “Claim”) against any Indemnitee to the extent such Claim alleges breach of data subjects’ rights resulting from a failure to comply with the provisions set forth in this DPA.

12.2. With the exception of the indemnification obligations of the Controller as set forth in Clause 12.1, the limitation of liability provisions as outlined in the Agreement shall apply to this DPA. Any liability arising under this DPA shall be calculated in aggregate with, and not in addition to, any liability arising under the Agreement. Furthermore, such liability shall be subject to the same limitations and exclusions as set forth in the Agreement.

13. MISCELLANEOUS

13.1. The DPA shall enter into force upon signature and shall remain in force for the duration of the Agreement or until the DPA is terminated in accordance with the procedure set forth therein.

13.2. In the event of any conflict between the terms of this DPA and other terms and conditions between the Parties, the provisions of the following documents (in order of precedence) shall prevail: (a) the Standard Contractual Clauses; (b) this DPA; (c) the Agreement.

Annex 1

1. Subject Matter of the Processing

This Annex describes the nature and purpose of the data processing activities to be performed by the Processor on behalf of the Controller. The Processor provides multi-cloud Infrastructure deployment and management services.

2. Duration of the Processing

The Processor shall process Personal Data during the term of the Agreement and this DPA, and shall retain or delete such data pursuant to the Controller's instructions or as otherwise required by Applicable Law.

3. Categories of Personal Data

Given that the Processor does not have visibility into the exact types of data the Controller processes, the below list is illustrative and non-exhaustive. Actual data content is solely determined by the Controller.

- Potentially Personal Data (as provided by the Controller) may include:
  - Basic contact details (e.g., names, email addresses, phone numbers)
  - Employment information (e.g., job titles, IDs, performance data)
  - Financial information (e.g., payment details, credit card data)
  - Online identifiers (e.g., IP addresses, device IDs, location data)
  - Any other personal data uploaded by the Controller or its end users, which may include special categories of data if chosen by the Controller.

The Controller acknowledges its responsibility to ensure that any Personal Data or special categories of data it uploads, processes, or stores using the hosting services are handled lawfully in accordance with applicable Data Protection Law.

4. Categories of Data Subjects

Since the Processor does not monitor or determine the personal data within its Services, the below categories are provided as examples and are not intended to be exhaustive:

- Employees, agents, contractors, or other staff of the Controller
- Clients, customers, or prospective customers of the Controller
- Website visitors, end users, or other third-party individuals whose personal data is uploaded by the Controller
- Any other individuals whose personal data is provided to the Processor by the Controller

5. Special Categories of Data (If Applicable)

If the Controller intends to process any special categories of Personal Data (e.g., health data, biometric data, data relating to racial or ethnic origin, political opinions, religious beliefs), the Controller must inform the Processor in advance if additional or stricter security measures are required.

The Processor shall not be responsible for identifying whether special categories of data are being processed; the Controller assumes such responsibility as the party that uploads or otherwise makes the data available.

The Controller shall ensure that the processing of special categories of data via the Services is done in compliance with all applicable laws, regulations, and guidance, including but not limited to obtaining any required consents or implementing appropriate safeguards.

6. Acknowledgment

Each party acknowledges that the above description accurately reflects, to the extent reasonably possible, the categories of Personal Data and Data Subjects processed, the nature of the processing, and any special considerations. However, the Processor does not monitor, control, or assume responsibility for the data types the Controller chooses to store or transmit.

Annex 2

Technical and Organizational Measures

The Processor should implement the following technical and organizational measures to ensure a level of security appropriate to the risk associated with the processing of personal data:

I. Organizational Measures

1. **Confidentiality Obligations**
    - Employees and contractors should be bound by confidentiality agreements and should receive training on the importance of maintaining data confidentiality.
2. **Incident Response Plan**
    - The Processor should have a plan in place to promptly address and mitigate the effects of any personal data breaches or security incidents.
3. **Staff Training and Awareness**
    - Employees involved in processing personal data should receive appropriate training on data protection laws and security practices.
4. **Policy and Procedure Documentation**
    - The Processor should maintain up-to-date policies and procedures related to data protection and information security.
5. **Data Protection by Design and Default**
    - The Processor should consider data protection and privacy considerations during the design and implementation of processing systems and practices.
6. **Risk Assessment**
    - The Processor should perform regular risk assessments to identify and address potential vulnerabilities in data processing activities.
7. **Change Management**
    - Changes to processing systems and practices should be managed and documented to maintain security and compliance.

II. Technical Measures

1. **Access Control**
    - *Physical Access*: The Processor should control physical access to data centers and offices where personal data is processed, ensuring that unauthorized individuals cannot gain access.
    - *Logical Access*: Access to systems processing personal data should be restricted to authorized personnel through authentication mechanisms such as passwords and user IDs.
2. **Data Encryption**
    - Personal data should be encrypted during transmission over public networks and stored encrypted where appropriate to protect against unauthorized access.
3. **Network Security**

- Firewalls and intrusion detection systems should be used to protect networks containing personal data from unauthorized access and threats.

4. **Use of Technology Standards**

   - Industry-standard security technologies and practices should be used to protect personal data.

5. **Physical Security Measures**

   - Facilities should be equipped with appropriate security measures such as access controls, surveillance systems, and environmental controls.