Annex no. 2 to the Terms and Conditions

DATA PROCESSING ADDENDUM

version effective as of 2024-09-01

I. Definitions

1. Unless otherwise indicated, capitalized terms in this Data Processing Addendum shall have the meaning given to them in the Terms and Conditions.
2. The following terms and expressions used in this Data Processing Addendum, when capitalized, shall have the meanings assigned to them in this section:
   a) **„DPA"** means this Data Processing Addendum;
   b) **„Controller"**, **„Member State"**, **„Process/Processing"**, **„Processor"**, **„Special Categories of Personal Data"**, **„Personal Data"**, shall have the same meaning as defined in GDPR;
   c) **„GDPR"** means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data;
   d) **„Data Subject Request"** means a request from a Data Subject to exercise applicable rights under GDPR;
   e) **„Data Subject"** means an identified or identifiable natural person;
   f) **„Further Processor"** – means the entity used by the Service Provider in exercising the rights and obligations set out in the Terms and Conditions, the Service Agreements and the DPA in connection with the performance of certain Processing activities, which will have access to Personal Data;
   g) **„Notice of Further Processor"** – means a notice of intention to entrust the Processing of Personal Data by Service Provider to another entity other than those specified in Annex C to the DPA, containing: the name and registered office address of the Further Processor, the location where the Personal Data is processed, and the purpose of the further entrusting the Processing of Personal Data (the function of the Further Processor);
   h) **„Party"** means Entrepreneur or Service Provider;
   i) **„Entrepreneur"** means a Beneficiary who is a trader who has entered into a Service Agreement with a Service Provider; "
   j) **„Security Breach"** means a breach of security leading to any unauthorized, accidental or unlawful destruction, loss, alteration, disclosure of, or access to Personal Data which has been validated by the Service Provider;
   k) **„Supervisory Authority"** means an appointed government entity with the authority to enforce GDPR, including, an independent public authority which is established by a Member State pursuant to the GDPR.

II. Subject matter of the DPA

1. The Entrepreneur entrusts the Service Provider with the processing of Personal Data of which it is the Controller.
2. The Entrepreneur entrusts the Service Provider with the Processing of Personal Data in connection with the conclusion of the Service Agreements and the performance of the Services described therein, and the Service Provider accepts this task.

3. The Service Provider may only process Personal Data in order to fulfil its obligations under the Service Agreements.
4. The Service Provider may process Personal Data only for the duration of the Service Agreements and for the period from the termination or expiry of the Service Agreements until the deletion of the Personal Data in accordance with the provisions of the DPA, unless the Parties agree on a different term Processing of Personal Data under a separate agreement.
5. The DPA, the Terms and Conditions and the Service Agreements constitute the Entrepreneur's documented instructions to the Service Provider regarding the Processing of Personal Data.
6. The nature and purpose of the Processing, as well as the types of Personal Data and the categories of Data Subjects whose Personal Data will be Processed under the DPA, are detailed in Annex A to the DPA.

III. Obligations of the parties

1. The Entrepreneur undertakes:
   a) disclose Personal Data to the Service Provider only for one or more specified purposes that are in accordance with the Service Agreements,
   b) process the Personal Data and entrust it to the Service Provider only in accordance with the requirements of the GDPR or other applicable data protection law;
   c) be solely responsible for the accuracy, quality and lawfulness of the Personal Data and for the means by which the Entrepreneur obtained the Personal Data;
   d) where required to do so under the GDPR, ensure that Data Subjects have received and will receive a notice informing them that their Personal Data will be disclosed to the Service Provider or other entities designated by the Service Provider;
   e) not disclose any specific categories of Personal Data to the Service Provider.
2. The Service Provider undertakes to:
   a) to process Personal Data only on behalf of the Entrepreneur and in accordance with the Entrepreneur's reasonable instructions as detailed in this DPA;
   b) not process the Personal Data in a manner incompatible with the purposes indicated in the Service Agreement or for a longer period than is necessary for those purposes,
   c) ensure that its personnel involved in the Processing of Personal Data have been informed of the confidential nature of the Personal Data, have received appropriate training in their duties and have entered into written confidentiality agreements;
   d) to the extent permitted by law, promptly notify the Business of the receipt of any request for disclosure of Personal Data by any authority, including governmental authorities and law enforcement agencies, make reasonable efforts to resist the request where possible, and limit the scope of disclosure to what is strictly necessary to respond to the request;
   e) taking into account the state of the art, the costs of implementation, the nature, scope and context of the Processing, as well as the seriousness of the risks and industry best practices, implement appropriate technical and organisational measures to protect Personal Data from Security Breaches, as indicated in Annex B of the DPA;
   f) taking into account the nature of the Personal Data Processing activities carried out and the information available in connection with the provision of the Services under the Services Agreements, assist the Entrepreneur in fulfilling the following obligations:
      - carrying out the Data Protection Impact Assessment by providing the Entrepreneur with the necessary information regarding the Processing of Personal Data on the Service

Provider's ICT Systems needed by the Entrepreneur to carry out the Data Protection Impact Assessment;

- responding to the Data Subject's Request by providing the Entrepreneur with information on any requests sent directly to the Service Provider;
- reporting the Security Breach to the Supervisory Authority and notifying the Data Subjects of the Security Breach.

IV. Sub-processing

1. The Entrepreneur consents to the use of Sub-Processors by the Service Provider in the Processing of Personal Data for the purpose of proper provision of the Services under the Service Agreements, including the provision of certain functionalities and security of the Service Provider's ICT Systems.
2. The consent indicated in paragraph 1 above shall also apply to the transfer of Personal Data by the Service Provider to entities established outside the European Economic Area, provided that the Personal Data is transferred to a country providing an adequate level of protection in accordance with the provisions of Chapter V of the GDPR Regulation.
3. The list of Further Processors used or intended to be used by the Service Provider as of the commencement date of the DPA is set forth in Annex C to the DPA. By entering into the DPA, the Customer accepts entrusting the Processing of Personal Data to the entities specified in Annex C to the DPA.
4. If the Service Provider intends to use the services of Further Processors other than those indicated in Annex C to the DPA, the Service Provider shall provide the Entrepreneur with information about the Further Processor at least 14 days prior to the further entrustment of Personal Data Processing. Information about the Further Processor will be provided electronically to the Entrepreneur's email address. An amendment to Annex C does not require an amendment to the DPA.
5. Within 14 days of receipt of the Further Processor Notice, the Entrepreneur may object to the Further Processor. If an objection is not raised, the Entrepreneur shall be deemed to have agreed to the planned changes.
6. The submission of an objection to a Further Processor, depending on the type of services provided by the Further Processor, shall mean:
   a) termination of the Service Agreements with effect at the end of the month following the month in which the objection is made, if the entrustment of the Processing of Personal Data to the Further Processor is necessary for the provision of all Services in accordance with the Service Agreement and the Entrepreneur is not able to use a specific Service or a specific functionality; or
   b) the Entrepreneur ceases to use a particular Service or functionality, or is unable to access a particular Service or functionality, the operation of which involves the use of a Further Processor, where the entrustment of Personal Data Processing to the Further Processor is only necessary for the provision of a particular Service or functionality.

During the termination period of the Service Agreements, the Service Provider shall not transfer Personal Data to the Further Processor for processing.

7. The agreement between the Service Provider and the Further Processor shall impose on the Further Processor the same data protection obligations as set forth in the DPA, in particular the obligations to comply with the provisions of the relevant law, including obligations to apply technical and organizational measures that will be adequate to the type of entrusted Personal Data

and the risk of violation of the rights or freedoms of Data Subjects. Rights of Further Processors shall not be broader than those of the Service Provider specified in the DPA.

8. The Service Provider shall be liable for the acts and omissions of the Further Processors.

V. Security Breach

1. In the event that the Service Provider identifies a Security Breach, in accordance with the Service Provider's established procedure, the Service Provider shall notify the Entrepreneur of such Security Breach immediately, but no later than within 36 hours of the discovery of the Security Breach, unless such notification is delayed or prohibited by an act or order of a Supervisory Authority.
2. Information on a Security Breach shall be sent by the Service Provider to the Entrepreneur's e-mail address.
3. In the event of a Security Breach, the Service Provider will immediately take all necessary technical and organisational measures to rectify the Security Breach and minimise its possible negative consequences.
4. The Service Provider shall cooperate with the Entrepreneur, to the extent reasonably practicable, in connection with any notifications to Supervisory Authorities or affected Data Subjects that are required in connection with the Security Breach, insofar as this is relevant to the Service Provider's Processing of Personal Data under this DPA.

VI. Other information obligations

1. The Service Provider shall inform the Entrepreneur immediately, but no later than within 5 working days:
   a) of any proceedings, in particular administrative or judicial, relating to the Processing of Personal Data, any administrative decision or court ruling concerning the Personal Data addressed to the Service Provider, as well as any planned proceedings or ongoing checks and inspections relating to the Processing of Personal Data;
   b) if it considers that the instructions given to the Service Provider by the Entrepreneur regarding the Processing of Personal Data constitute a breach of the law on the protection of Personal Data, in particular the GDPR;
2. At the request of the Entrepreneur, the Service Provider shall promptly provide any information necessary to demonstrate compliance with the obligations set out in the DPA or the applicable law.

VII. Control of Processing

1. The Entrepreneur shall be entitled to control the Processing of the Personal Data entrusted to the Service Provider personally, by its employees or by an auditor authorised by the Entrepreneur.
2. The audit, control or inspection may be carried out in the form of an undertaking to provide the Entrepreneur with all information relating to the Processing of Personal Data, without delay, but no later than 10 working days from the date of receipt of such request from the Entrepreneur.
3. The Entrepreneur undertakes to ensure that the audit will be carried out with respect for the secrecy of the Service Provider's business and, in particular, that the persons carrying out the audit activities will be obliged to keep confidential any information they obtain in connection with the audit.
4. The Entrepreneur also undertakes to ensure that the persons carrying out the activities covered by the audit are not employed, are not partners, shareholders or members of the bodies of entities carrying out activities competitive to the business activities carried out by the Service Provider.

5. The Service Provider shall have the right to require the Entrepreneur to conclude a confidentiality agreement in connection with the intention to carry out the audit.
6. The Entrepreneur and any persons performing audit activities may furthermore be bound to confidentiality in relation to the Further Processor.
7. The Entrepreneur undertakes to ensure that the audit is carried out without prejudice to the continuity of the Service Provider's business.
8. The Entrepreneur shall be liable for damages caused to the Service Provider in connection with a breach by the Entrepreneur or persons carrying out the activities covered by the audit of the provisions of paragraphs 2 - 6 above, including the Service Provider's lost profits.
9. The Entrepreneur shall bear the costs of the audit, in particular the costs related to the use of an external professional auditor.
10. If the Entrepreneur identifies objections to the Processing of Personal Data by the Service Provider or Further Processors, the Entrepreneur will be entitled to make recommendations to the Service Provider.

VIII. Termination of the Processing of Personal Data

1. Upon termination or expiry of the Service Agreements, the Service Provider shall delete the Personal Data provided by the Entrepreneur in accordance with the Service Agreement without delay and no later than within 30 days.
2. The above requirement shall not apply to the extent the Service Provider is required by applicable law to which Service Provider is subject, to retain some or all Personal Data and as part of Service Provider’s standard archival or backup systems, provided that such Personal Data shall continue to be subject to the provisions of this DPA. In such case the relevant Personal Data shall be securely isolated and protected from any further Processing, except to the extent required by applicable law.

IX. Final Provisions

1. The DPA is entered into for the duration of the Service Agreements.
2. The DPA shall be governed by the law applicable to the Service Agreements.

ANNEXES:

Annex A Details of the processing
Annex B List of technical and organisational measures
Annex C List of further processors

ANNEX A: PROCESSING DETAILS

Nature and purpose of processing	Providing the Services to the Entrepreneur.
Categories of Data Subjects	Employees of the Entrepreneur, authorised to use the Services, potential customers, contractors or their employees, associates
Types of Personal Data	business email address, IP address, name, business telephone number, affiliation with the Entrepreneur, position, image, correspondence, personal data contained in documents collected in the Application
Special Categories of Personal Data transferred	Not applicable.
Duration of Processing	For the duration of the Agreement, and subject to local legal requirements.
Frequency of transfer	Continuous basis for the duration of the Agreement.
Transfers to Further Processors	As described above.

ANNEX B: TECHNICAL AND ORGANISATIONAL MEASURES

I. SECURITY OF PERSONAL DATA

1. Organisational safeguards:
   The Service Provider has an Information Security Policy that governs the protection of Personal Data, including a policy for managing Security Breaches.
2. Physical safeguards:
   The Service Provider has dedicated secure areas where Personal Data is Processed.
3. Security measures regarding access control:
   The Service Provider has a policy for strong passwords, changing passwords and locking accounts.
4. Operational security measures:
   a) The Service Provider's ICT systems and applications used to Process Personal Data are regularly updated, verified for vulnerabilities and protected with anti-virus systems;
   b) The Service Provider uses protection against unauthorised access to systems and networks through firewalls.

II. SECURITY OF SYSTEMS

1. The security features of the Service Provider's systems have been selected based on best security practices.
2. Authentication security: identity verification is used during communication to ensure that only authorised parties can be authenticated and that credentials are securely stored and transmitted.
3. Access control security: those gaining access have valid authorisations and users are associated with specific sets of roles and permissions.
4. Error handling and logging safeguards: mechanisms are in place to log security incidents, and all logged information is processed and stored securely.
5. Safeguards for data protection mechanisms: it is ensured that data is protected against unauthorised viewing or disclosure, both during transmission and during storage. Data shall be protected against malicious creation, alteration or deletion by unauthorised persons and shall only be accessible to authorised users when needed.
6. Communication security: a secure connection is used for all connections (external and internal) that are authenticated or involve sensitive data or functions; mechanisms are provided to prevent degradation of connection security.

Annex C: List of Further Processors

No.	Name of Further Processor	Address of the Further Processor	Place of processing by the Further Processor	Purpose of the further entrustment
1	Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855, Luxembourg	Frankfurt, Germany	IT Cloud services
2	Cloudflare, Inc.	101 Townsend St, San Francisco, CA 94107, USA	EEA, USA and other countries (see their privacy policy)	IT Cloud services, Content Delivery Network
3	Neon Inc.	209 Orange Street, City of Wilmington, County of New Castle, Delaware 19801, USA	Frankfurt, Germany (AWS)	Database

1. Amazon Web Services EMEA SARL
    a) Privacy Policy: https://aws.amazon.com/privacy/
    b) DPA: https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf
2. Cloudflare, Inc:
    a) Privacy Policy: https://www.cloudflare.com/privacypolicy/
    b) DPA: https://www.cloudflare.com/cloudflare-customer-dpa/
3. Neon Inc.:
    a) Privacy Policy: https://neon.tech/privacy-policy
    b) DPA: https://neon.tech/dpa