Data Processing Addendum

This Data Processing Addendum (**DPA**) forms part of the electronic agreement for the purchase of the Vendor Service as identified in such agreement ("**Principal Agreement**") between: (i) Quality Unit, s.r.o., Vajnorská 100/A, 83104 Bratislava, Slovakia (European Union) **("Vendor"** or **"Data Processor")** and (ii) [insert your company legal name and address] (**"Company"** or **"Data Controller"**). Data Controller and Vendor are each a **"Party"** and collectively, the **"Parties"**.

Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that:

The terms and conditions set out below shall be added as an addendum to the Principal Agreement.

Except where the context requires otherwise, references in this DPA to the Principal Agreement are to the Principal Agreement as amended by, and including, this DPA.

DEFINITIONS AND INTERPRETATION

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

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

The terms, "**Commission**", "**Controller**", "**Processor**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly;

"Company**'s Personal Data**" means any Personal Data Processed by a Processor on behalf of Data Controller pursuant to or in connection with the Principal Agreement;

"**Standard Contractual Clauses**" the European Commission's Implementing Decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to processors established in third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council;

"**Subprocessor**" means any person appointed by or on behalf of Vendor to Process Personal Data on behalf of Company in connection with the Principal Agreement; and

'**International Organisation**' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries (see Article 4(26) of the GDPR);

'Appropriate Safeguards' means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under the applicable data protection laws from time to time.

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

Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement.

1. PROCESSING OF COMPANY PERSONAL DATA

1.1. **Role of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Personal Data, Company is the Controller, Vendor is the Processor and that Vendor will only engage Subprocessors pursuant to the requirements set out in Clause 5 Subprocessors below.

1.2. **Data Controller's Processing of Personal Data.** Data Controller shall, in its use of the Services and instructions to Vendor:

a) comply with all applicable data protection laws in the Processing of Company Personal Data; and

b) have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which Company acquired Personal Data.

c) without prejudice to Vendors's security obligations in Section 1.3 of this DPA, Company acknowledges and agrees that it, rather than Vendor, is responsible for certain configurations and design decisions for the services and that Company , and not Vendor, is responsible for implementing those configurations and design decisions in a secure manner that complies with applicable Data Protection Laws. Explicitely connecting, feeding and securing integrations for inputs and outputs.

1.3. **Vendor's Processing of Personal Data.** Vendor shall:

a) comply with all applicable data protection laws in the Processing of Company Personal Data and shall not by any act or omission cause Company (or any other person) to be in breach of any applicable data protection laws; and

b) treat Personal Data as Confidential Information; and

c) Process and shall ensure each person acting under its authority shall Process Company Personal Data only on the relevant Company's documented instructions unless Processing is required by applicable laws to which the relevant Processor is subject, in which case Vendor shall to the extent permitted by applicable laws inform Company of that legal requirement before the relevant Processing of that Personal Data, and

d) immediately inform Company in writing if, in the Vendor's opinion, a Processing instruction infringes the applicable data protection laws or any other applicable laws relating to data protection and explain the reasons for its opinion, provided that this shall be without prejudice to clause 2.3.a).

1.4. **Purposes of Processing.** Company instructs Vendor (and authorises Vendor to instruct each Subprocessor) to Process Company Personal Data for the provision of the Services and consistent with the Principal Agreement;

1.5. Details of the Processing. Annex 1 to this DPA sets out certain information regarding the Processors' Processing of the Company Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other applicable data protection laws).

2. DATA SUBJECT RIGHTS

2.1. **Data Subject Request**. Vendor shall, to the extent legally permitted, promptly (and in any event no later than 2 working days within the receipt of the request) notify Company if Vendor or Vendor's Subprocessor receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("**Data Subject Request**").

2.2. **Vendor Assistance**. Taking into account the nature of the Processing, Vendor shall assist Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company's obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the applicable data protection laws. In addition, to the extent Company, in its use of the Services, does not have the ability to address a Data Subject Request, Vendor shall, at its cost and expense, and upon Company's request provide commercially reasonable efforts to assist Company in responding to such Data Subject Request, to the extent Vendor is legally permitted to do so and the response to such Data Subject Request is required under applicable data protection

laws. In any event, Vendor shall not respond to any Data Subject Request without Company's prior written approval.

3. VENDOR PERSONNEL

3.1. **Confidentiality**. Vendor shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Vendor shall ensure that confidentiality obligations regarding Personal Data survive the termination of the personnel engagement.

3.2. **Reliability**. Vendor shall take commercially reasonable steps to ensure the reliability of any Vendor personnel and Vendor Subprocessor personnel who may have access to the Company Personal Data.

3.3. **Limitation of access.** Vendor shall ensure in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with applicable laws in the context of that individual's duties to Vendor.

4. SUBPROCESSING

4.1. **Appointment**. Company authorises Vendor to appoint (and permit each Subprocessor appointed in accordance with this Clause 4 to appoint) Subprocessors in connection with the Services and in accordance with this Clause 5 and any restrictions in the Principal Agreement.

4.2. **Current Subprocessors**. Vendor shall make available to Company the current list of Subprocessors for the Services, including the identities of those Subprocessors and their country of location in Annex 3. Vendor may continue to use those Subprocessors already engaged by Vendor as at the date of this DPA, subject to Vendor in each case as soon as practicable meeting the obligations set out in this Clause 4. Current list of subprocessors is available on www.flowhunt.io/privacy-policy/subprocessors/.

4.3. **New Subprocessors**. Vendor shall give Company prior written notice of the appointment of any new or replacement Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 10 days of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment:
Vendor shall work with Company in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; and where such a change cannot be made within 30 days from Vendor's receipt of Company's notice, notwithstanding anything in the Principal Agreement, Company may by written notice to Vendor with immediate effect terminate the Principal Agreement to the extent that it relates to the Services which require the use of the proposed Subprocessor.

5. SECURITY

5.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Vendor shall, at its cost and expense, in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in the applicable data protection laws, especially Article 32 of the GDPR. In assessing the appropriate level of security, Vendor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5.2. These measures should entail physical, logical and data access control as well as data transfer, instruction, entry, availability and separation control. Vendor shall upon request provide Company with an overview of all such measures. Vendor agrees and warrants that it has implemented the technical and organisational security measures specified in Annex 2 before processing the personal data transferred.

5.3. Vendor will not materially decrease the overall security of the Services during a subscription term.

6. PERSONAL DATA BREACH

6.1. Vendor shall notify Company without undue delay but in any event no later than 36 hours after Vendor or any Subprocessor becomes aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow Company to meet its obligations to report or inform Data Subjects of the Personal Data Breach under the applicable data protection laws.

6.2. Such notification shall as a minimum:

a) describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

b) communicate the name and contact details of Vendor's data protection officer or other relevant contact from whom more information may be obtained;

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

d) describe the measures taken or proposed to be taken to address the Personal Data Breach.

6.3. Vendor shall, at its cost and expense, co-operate with Company and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7. RECORDS, INFORMATION AND AUDIT

7.1. Vendor shall make available to Company on request in a timely manner and in any event within 3 working days copies of complete, accurate and up to date written records of all categories of Processing activities carried out on behalf of Company, containing such information as Company reasonably requires to demonstrate Vendor's and Company's compliance with their respective obligations under applicable data protection laws and this DPA.

7.2. Vendor shall upon reasonable notice and at no cost to Company allow for and contribute to audits, for the purpose of demonstrating compliance by Vendor and Company with their respective obligations under applicable data protection laws and under this DPA. Especially, Vendor shall provide and procure reasonable access (where practicable, during normal business hours) to information, documentation, facilities, equipment, premises and sites relating to Company Personal Data and/or the records referred to in clause 7.1, and to Vendor Personnel.

7.3. Vendor shall promptly resolve, at its own cost and expense, all data protection and security issues discovered by Company and reported to Vendor that reveal a breach or potential breach by Vendor of its obligations under this DPA.

7.4. If Vendor is in breach of its obligations under this DPA, Company may suspend the transfer of Company Personal Data to Vendor until the breach is remedied.

7.5. Company shall be entitled to share any notification, details, records or information provided by or on behalf of Vendor under this DPA with Company, its professional advisors and/or the Supervisory Authority.

8. DELETION OR RETURN OF COMPANY PERSONAL DATA

8.1. Vendor shall (and shall ensure that all persons acting on its behalf and all Vendor Personnel shall) without delay and in any event within 5 business days, at Company's written request, either certifiably delete or destroy in a secure and definite/irreversible manner or securely return all originals, copies, reproductions and summaries of Company Personal Data

Processed by Vendor and its Subprocessors to Company in such form as Company reasonably requests after the earlier of:

a) the end of the provision of the relevant Services related to Processing of such Personal Data; or
b) once Processing by the Supplier of any Personal Data is no longer required for the purpose of the Supplier's performance of its relevant obligations under this Agreement,

and certifiably delete or destroy in a secure and definite/irreversible manner existing copies (unless storage of any data is required by applicable law and, if so, Vendor shall inform Company of any such requirement).

9. INDEMNITY

9.1. Vendor agrees to indemnify and keep indemnified, and defend at its own expense, Company against claims, damages or expenses incurred by Company or for which Company may become liable due to any failure by the Vendor or its employees or agents to comply with any of its obligations under this DPA. Liability is limited to the amount of Company's average monthly payment for the Services.

10. TRANSFER MECHANISMS

10.1. In the absence of an adequacy decision, Company Personal Data may only be transferred to a third country or an International Organisation outside the EEA where there are Appropriate Safeguards. Such transfer (and any onward transfer) shall:

a) be pursuant to a written contract, including equivalent obligations on the Subprocessor in respect of Company Personal Data as apply to Vendor under this DPA;
b) is effected by way of Appropriate Safeguards and, where practicable, the form of these shall be subject to Company's prior written approval;
c) otherwise complies with applicable data protection laws.

GENERAL TERMS

11. Warranty as to Authority

11.1. Each person signing this DPA hereby represents and warrants that he or she has full authority to execute this Agreement for the Party on whose behalf he or she is signing.

12. Governing Law and Jurisdiction

12.1. Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses: the Parties to this DPA hereby submit to Slovak courts, including disputes regarding its existence, validity or termination or the consequences of its nullity; and this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of Slovakia.

13. Order Of Precedence

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

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above, save for the provisions introduced by the GDPR that became effective from 25th May 2018.

[Company]

Signature _____

Name _____

Title _____

Date Signed _____

Quality Unit, s.r.o.

Signature _____

Name: Viktor Zeman

Title CEO

Date Signed _____

ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Company Personal Data

The subject matter and duration of the Processing of the Company Personal Data are set out in the Principal Agreement and this DPA. The duration of the processing of Company Personal Data equals the duration of use of the Service.

The nature and purpose of the Processing of Company Personal Data

Provide customer services related to the Service.

The types of Company Personal Data to be Processed

Account owner - Name, Email, IP Address, Cookies, Logs, Payment information, Additional information collected by Data controller stored in their account.

Employees - Name, Email, IP Address, Cookies, Logs, Additional information collected by Data controller stored in their account.

End users of the Services - Name, Email, IP Address, Cookies, Additional information collected by Data controller stored in their account.

The categories of Data Subject to whom the Company Personal Data relates

Account owner, Employees, End users of the Services

The obligations and rights of Company

The obligations and rights of Company are set out in the Principal Agreement and this DPA.

ANNEX 2: TECHNICAL AND ORGANISATIONAL SECURITY

Vulnerability Scans
Vendor performs both external and internal vulnerability scans. External scans include looking for ways in which malicious outsiders can exploit the Vendor and the Service, and internal scans include looking for threats inside the organisation, such as the potential for privilege abuse.

Penetration Testing
Vendor employs a professional penetration testing team which performs a controlled form of hacking in which they work on behalf of the Vendor, use the same techniques as a criminal hacker to search for vulnerabilities in the Service or other Vendor applications.

Security Audit
Vendor is a subject to security audits performed by companies specialized in security audits for cloud software products.

Access Control Management

- Ensure that role-based access rights management is in place together with the implementation of procedures to maintain a need-to-have; need-to-know basis during provisioning. Ensure timely revocation of leaver's accounts together with protecting all access to business information via secure log-on procedures.
- Ensure Access rights are approved prior to assignment and are reviewed periodically.
- Ensure only authorized personnel has access to process the personal data of the Company. The access is limited via unique username, password and enabled 2FA.

Entry control

- Ensure only authorised persons are given access to the office premises of the Vendor. The access is granted on issuing and registering the access cards. The access cards are regularly evaluated and checked.
- The security of data centers is ensured via 24/7 manned security, CCTV video surveillance, multifactor identification and security breach alarms.

Asset Management

- Ensure that an asset inventory is in place for all assets, identifying owner and location of assets.

Cryptography

- Ensure that storage of sensitive information such as passwords of users is done by using strong hashing cryptographic primitives such as hashing with salted values.
- Ensure that the transmission of client information is done via HTTPS using industry recommended protocols.

Operational Security

- Ensure that adequate backup, backup testing and restore procedures are in affect.
- Ensure Information is backed up, and backups are regularly tested to ensure availability of Personal Data.
- Ensure that any information that is backed up and taken off site, is encrypted.

Incident Management

- Ensure proper information security incident management policies and procedures are in place detailing step-by-step processes on how incidents are dealt with, documented and communicated.
- Ensure proper classification guidelines are implemented to distinguish between incidents affecting availability of Personal Data and incidents affecting the confidentiality, integrity and availability of information.

Communications Security

- Transfer of Information is encrypted using secured HTTPS protocol.
- Maintain encryption (using industry recommended protocols and ciphers) during any Information transferred over the internal network, as well as any transmission of client information.

Vulnerability Management

- Ensure both external and internal vulnerability scans are performed. External scans include looking for ways in which malicious outsiders can exploit the Vendor and the Service, and internal scans include looking for threats inside the organisation, such as the potential for privilege abuse.
- Ensure a professional penetration testing team which performs a controlled form of hacking in which they work on behalf of the Vendor, use the same techniques as a criminal hacker to search for vulnerabilities in the Service or other Vendor applications.
- Ensure the Vendor is a subject to security audits performed by companies specialized in security audits for cloud software products.

ANNEX 3: ADDITIONAL DETAILS REGARDING SUBPROCESSORS

Quality Unit, s.r.o. provides its Service (referred to here as "FlowHunt") to You through its web site located at www.flowhunt.io/privacy-policy/ (URL of your account). Quality Unit, s.r.o. uses certain subprocessors to assist it in providing the FlowHunt Service.

What is a Subprocessor

A subprocessor is a third party data processor engaged by FlowHunt, who has or potentially will have access to or process Service Data (which may contain Personal Data). FlowHunt uses various types of sub-processors to perform different functions as explained in the tables below.

Due Diligence

FlowHunt undertakes to use a commercially reasonable selection process by which it evaluates the security, privacy and confidentiality practices of proposed subprocessors that will or may have access to or process Service Data.

FlowHunt owns or controls access to the infrastructure that FlowHunt uses to host Service Data submitted to the Services, other than as set forth below. Currently, the FlowHunt production systems for the Services are located in co-location facilities in the United States and Europe.

Customer accounts are established in one of these regions based on where the Customer is located; the Customer's Service Data subsequently remains in that region unless agreed between Customer and FlowHunt, but may be shifted among data centers within a region to ensure performance and availability of the Services. The following table describes the countries and legal entities engaged in the storage of Service Data by FlowHunt.

Subcontracting company	Data center location	Service
Client-specific subprocessors		
Amazon Web Services, Inc.	Germany	Infrastructure subprocessor – Servers Data center facilities

Vendor-specific subprocessors		
Subcontracting company	**Company location**	**Service**
AiMingle, s.r.o.	Czech Republic	Other subprocessor - Services AiMingle, s.r.o. a Quality Unit member entity. Quality Unit, LLC functions as a subprocessor to provide the FlowHunt Service.
Quality Unit, LLC	United States	Other subprocessor - Services Quality Unit, LLC is a Quality Unit member entity. Quality Unit, LLC functions as a subprocessor to provide the FlowHunt Service.
Quality Unit Ukraine, LLC	Ukraine	Other subprocessor - Services Quality Unit Ukraine functions as a subcontractor to provide the FlowHunt Service.
Makara Partner, s. r. o.	Slovakia	Our accounting may access Service Data in order to create and process invoices.

Service-specific subprocessors		
Subcontracting company	**Company location**	**Service**
OpenAI	United States	Other subprocessor - LLM Services Service protected by signed DPA amendment between OpenAI and Vendor. Optional - Client can choose to use the service for task processing, content generation, data analysis, and automation.

Groq	United States	Other subprocessor - LLM Services Optional - Client can choose to use the service for task processing, content generation, data analysis
XAI	United States	Other subprocessor - LLM Services Service protected by signed DPA amendment between OpenAI and Vendor. Optional - Client can choose to use the service for task processing, content generation, data analysis, and automation.
Google Cloud Platform	United States	Other subprocessor - LLM Services Service protected by signed DPA amendment between Google and Vendor.
Anthropic AI	United States	Other subprocessor - LLM Services Optional - Client can choose to use the service for task processing, content generation, data analysis