Data Processing Agreement
(controller to processor),
dated _____, 20__

[name of the counterparty], established and existing in accordance with the legislation of [name of the country], represented by [job title and full name of the authorized person], acting under [the basis of authority], hereinafter referred to as the "Controller", on the one hand, and

Huntflow AM, LLC, established and existing in accordance with the legislation of Republic of Armenia, represented by Director M.Tansky, acting under Articles of Association, hereinafter referred to as the "Processor" on the other hand, and

jointly referred to as the "Parties", have entered into this Data Processing Agreement as follows

1. **General provisions**

Based on Article 28 of the General Data Protection Regulation of April 27, 2016 (EC) 2016/679 ("GDPR"[1]), hereinafter referred as "applicable law in the field of processing and ensuring the security of personal data", the Controller instructs the Processor regarding the processing of personal data, which includes [specify the list of operations with personal data (e.g. collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction)], with or without automation, in accordance with the terms of the Data Processing Agreement. The Controller has the right to send additional instructions to the Processor on the processing and protection of personal data, and the Processor undertakes to follow them if they do not violate the requirements of applicable legislation.

2. **Terms and definitions**

The following terms and definitions shall be used for the purposes of this Data Processing Agreement:
Personal data – any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, the processing of which is carried out by the Processor and (or) Sub-Processors on the basis of and pursuant to the Data Processing Agreement.
Personal data processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller – a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Processor – a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller, under instructions from the Controller for the purposes defined by the Controller.

Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

[1] General Data Protection Regulation 2016/679: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

3. Information about personal data processing

3.1 The Processor processes the personal data of the following categories of data subjects:

- [list of categories of data subjects].

3.2 The purposes of personal data processing are:

- [list PD processing purposes].

3.3 List of categories of personal data processed:

- [list categories of personal data].

3.4 Duration of personal data processing:

- [duration of personal data processing].

3.5 Methods for the transfer (provision, access) of personal data between the Parties:

- [method for the transfer of personal data].

4. Responsibilities of the Controller and Processor

4.1 The Controller is responsible for:

- providing information to the data subjects including about transferring personal data to the Processor;
- ensuring that processing of personal data has an appropriate legal basis and that the data subject's rights are fulfilled;
- carrying out data protection impact assessments (DPIA) in the case if high risk processing of personal data takes place;
- ensuring that appropriate security measures are taken;
- determining whether notification to data protection authorities and/or data subjects is necessary in case of a data breach.

4.1 The Processor is required to comply with:

- Documents and requirements on the personal data processing provided for by applicable law in the field of personal data processing and ensuring the security of personal data, including:
  - appoint an employee responsible for organizing the personal data processing;
  - exercise internal control and / or audit of the compliance of personal data processing with the applicable legislation in the field of personal data processing and ensuring the security of personal data and regulations adopted in accordance with it, policy regarding personal data processing, and local acts of Processor;
  - assist the Controller in ensuring that the Controller complies with the requirements of the applicable legislation in the field of personal data processing and ensuring the security of personal data;
  - publish or otherwise provide unrestricted access to the document defining the policy regarding the personal data processing to the information on the implemented requirements for the protection of personal data;
  - determine the list of employees (structural divisions) who are allowed to process the personal data;
  - familiarize employees directly involved in the processing of personal data with the provisions of the legislation in the field of processing and ensuring the security of personal data, including the requirements for the protection of personal data, documents determining the policy regarding the processing of personal data, local acts on the processing of personal data, and (or) train the employees;

- allow for the personal data processing only those employees who have confirmed their obligations to fulfill the requirements of this agreement and legislation in the field of personal data processing and ensuring the security of personal data;
- ensure compliance with principles of personal data processing provided in the Article 5 of the GDPR;
- assist the Controller by appropriate technical and organisational measures for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights indicated in the Articles 7, 12-18, 20-22, 34, 77 of the GDPR, and monitor the reception and processing of such requests;
- make available to the Controller all information necessary to demonstrate compliance with Article 28 of the GDPR;
- assist the Controller in carrying out a data protection impact assessment in case the personal data processing may lead to a high risk in relation to the rights and freedoms of the data subjects;
- inform the Controller of the intentions and reasons for the transfer of personal data to third parties and (or) international organizations strictly before the transfer of personal data;
- inform the Controller of any anticipated changes in the processing of personal data;
- inform the Controller of cases of violation of the applicable law in the field of personal data processing and ensuring the security of personal data;
- immediately inform the Controller if it considers that the instruction given to the Processor constitutes a breach of applicable legislation in the field of processing and ensuring the security of personal data legislation on data protection;
- immediately notify the Controller of the personal data breach after the Processor became aware of the personal data breach, with detailed information about the personal data breach provided in stages as more detailed information is received.

5. Requirements to ensure the security of personal data

5.1 Ensuring the security of personal data when processing them in personal data information systems should be ensured by fulfilling the requirements for the protection of processed personal data in accordance with applicable law in the field of personal data processing and security of personal data:

- application of organizational and (or) technical measures required pursuant to Article 32 of the GDPR to ensure the security of personal data during its processing, including in information systems of the Processor, necessary to ensure confidentiality, integrity, availability and authenticity of processes and (or) systems to protect personal data from unlawful or accidental access to them, destruction, modification, blocking, copying, providing, dissemination of personal data, as well as from other illegal actions in relation to personal data;
- ensuring the detection of unauthorized access to personal data and taking action;
- ensuring the recovery of personal data modified or destroyed due to unauthorized access to it;
- setting rules for access to personal data processed in the personal data information system, as well as ensuring that all actions performed with personal data are recorded in the personal data information system;
- ensuring control over measures taken to ensure the security of personal data;
- assisting the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to the Processor;
- organization of a security regime for the premises in which an information system is placed that prevents the possibility of uncontrolled entry or stay in these premises by persons who do not have access to these premises;
- ensuring the safety of personal data carriers.

6. Notification about personal data breach

6.1 The Processor shall notify the Controller if the Processor detects a personal data breach or if the Processor reasonably believes that there has been a personal data breach. The notification should include the following information:

- the date and time of the personal data breach was detected;
- the actual circumstances of the breach;
- the categories and approximate number of the data subjects concerned;
- the categories of personal data and approximate number of personal data records concerned;
- the Processor's information systems and personal data processing within the Data Processing Agreement affected by the personal data breach;
- the possible consequences of the personal data breach;
- the measures taken or proposed to be taken by the Processor to address personal data breach;
- any reports regarding the breach which was provided by the Processor to law enforcement and other authorized bodies;
- the contact details of a person who can provide detailed information on the personal data breach.

6.1 The initial notification of personal data breach shall be sent to the Controller no later than 24 hours from the time of detection of a personal data breach. Additional notifications containing new and (or) additional information about a personal data breach shall be provided to the Controller as soon as possible as such information becomes available.

6.2 The Processor shall not notify any individual or any third party of any personal data breach without the Controller's prior permission except to the extent required by the applicable legislation.

6.3 The Processor immediately takes all necessary measures to eliminate the threat to the security of personal data, to prevent any possible negative consequences for the data subjects, the Controller or to minimize the possible negative effects. The Processor carries out and documents the analysis of the reasons of a personal data breach and provides the Controller with the results of the analysis by request.

7. Responsibility

7.1. Responsibility to the data subject for the actions of the Processor is borne by the Controller.

7.2. The Processor shall be liable to the Controller of personal data.

7.3. The Processor is prohibited to involve other sub-processors for the implementation of the obligations imposed on it by this agreement for the processing of personal data without prior specific or general written authorisation of the Controller. If such permission has been obtained, the Processor shall execute written agreements with the sub-processors involved, ensuring that the level of protection of personal data is not lower than that provided for in this Data Processing Agreement. At the same time, the Processor undertakes to bear responsibility for the observance of the present provisions by the sub-processor as if the corresponding processing was carried out by the Processor.

7.4. The Party that has not fulfilled or improperly fulfilled any of the obligations under the Data Processing Agreement shall be liable in the amount of documented direct damage caused to the other Party in connection with and in the amount of the demands satisfied in accordance with judicial acts and (or) in the amount of the collected administrative and other fines.

8. Audits

8.1 Based on the Controller prior written notice, the Processor is obliged to provide all the information necessary to confirm compliance with the conditions set forth in this Data Processing Agreement, as

well as to allow the Controller and participate in audits, including inspections conducted by the Controller or other auditor, on behalf of the Controller.

8.1 At the Controller's choice, the audit can be conducted by means of a questionnaire. If it is the case, the Processor must provide the Controller with a completed questionnaire no later than 10 business days from the date of receipt of the questionnaire from the Controller.

8.2 If the Processor involves sub-processors for processing of personal data, the Controller shall be entitled with the right to audit the sub-processors. The Processor shall carry out its own audit of the sub-processors specified by the Controller. The results of such audit shall be documented by the Processor and provided to the Controller not later than 10 business days from the date of completion of the audit.

9. **Other provisions**

9.1 After the completion of the provision of the services, the Processor by Controller choice:

- return a full copy of all personal data to the Controller in the format specified by the Controller, using secure channels of information transfer, and destruction all other copies of personal data using means of guaranteed information destruction;
- destroy all copies of personal data using the means of guaranteed destruction of information.

9.1 This Data Processing Agreement is valid until the achievement of the purposes of personal data processing or may be terminated by the Parties on the terms set out in the Service Agreement.

9.2 This Data Processing Agreement is made in two copies, one for each of the parties having the same legal force.

Signatures of the Parties

Party 1	Party 2 / Сторона 2
Huntflow AM, LLC	[name of the Controller] / [наименование организации]
Armenia, YEREVAN, ARABKIR, 36 MANUSHYAN	[address of the Controller] / [адрес организации]
_____	_____
Director/ M.Tansky	[position of authorized person] / [full name]/ [должность ответственного лица] / [ФИО]