Data Management Agreement
(joint controllers),

dated __________, 20__

Parties to the agreement:

- 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;
- [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];
- [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 jointly as the “Joint Controllers” or “Parties”, and separately as the “Controller” or “Party”, have agreed as follows.

Based on Article 26(1) of the General Data Protection Regulation of April 27, 2016 (EC) 2016/679 (“GDPR”[1]), joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR.

1. General provisions

1.1. In accordance with Article 26(1) of the GDPR, if two or more controllers jointly determine the purposes and means of personal data processing, they are Joint Controllers.

1.2. Controllers agree that within the framework of [name of the processes], they are Joint Controllers.

1.3. This Agreement sets out the allocation of responsibilities between Controllers.

2. Terms and definitions

The following terms and definitions shall be used for the purposes of this Data Management 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.

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

Joint controller – a controller that jointly with one or more controllers determines the purposes and means of processing.

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.

3. Information about personal data processing

1.4. Joint Controllers process personal data of the following categories of data subjects:

- [list of categories of data subjects].

1.5. The purposes of joint processing of personal data are:

- [list PD processing purposes].

1.6. List of categories of personal data jointly processed:

- [list categories of personal data].

1.7. Duration of personal data processing:

- [duration of personal data processing].

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

- [method for the transfer of personal data].

4. General allocation of responsibilities

4.1. The Parties must clearly define their obligations and corresponding obligations to comply with the GDPR requirements.

4.2. The Parties determine the areas of responsibility based on the specifics of interaction and the requirements of applicable legislation in the field of processing and ensuring the security of personal data.

4.3. The Controllers jointly determine which of the Parties will be the contact point for handling data subjects' requests, provided that the data subjects can exercise their rights in accordance with the GDPR in relation to each individual Controller. Processing of data subjects' requests is regulated by clause 7 of this Agreement. The Party designated as the contact point for data subject's requests – [name of the counterparty], [postal address], [phone number], [email address].

4.4. If personal data is not received from the data subject, the Controller who received this personal data ensures that the data subject is informed accordingly.

4.5. Each of the Controllers is responsible for interaction with data subjects who initially provided personal data to one of the Controllers, including the following responsibilities:

- compliance with the principles of personal data processing;
- ensuring that there is the necessary legal basis for personal data processing;
- informing data subjects about the processing of personal data and data subjects' rights;
- ensuring the security of processed personal data;
- responding to data subjects' requests;
- ensuring the erasure of personal data when the purposes of their processing are achieved.

4.6. Controllers are obliged to inform each other about changes of a location where personal data is processed (for example, creation of new offices or branches). If this may lead to the transfer of personal data to other countries, the processing of personal data is carried out in accordance with section 12 of this Agreement.

4.7. The allocation of responsibilities between Controllers in accordance with this Agreement does not prevent supervisory authorities, within their jurisdiction, from exercising their powers in relation to each of the Controllers.

5. Principles and legal basis of personal data processing

5.1. The Controller receiving personal data is responsible for ensuring that there is a legal basis for personal data processing including providing evidences of using such a legal basis by request of a supervisory authority or data subjects. Legal basis for the processing of personal data are:

- [Consent – the data subject has given a consent to the processing of personal data for one or more specific purposes;
- Contract – processing of personal data is necessary for the performance of a contract to which the data subject is party or in order to take steps at the data subject' request prior to entering into a contract;
- Legal obligation – the processing of personal data is necessary to achieve the goals stipulated by international agreements or the law for the implementation and fulfillment of the functions, powers and duties assigned to the Controller by applicable law;
- Legitimate interest – the processing of personal data is necessary for the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child].

5.2. Each Controller is responsible for compliance with the following principles of personal data processing:

- lawfulness, fairness and transparency processing of personal data – Article 5(1)(a) GDPR;
- processing of personal data for specified, explicit and legitimate purposes (purpose limitation – Article 5(1)(b) GDPR);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation – Article 5(1)(c) GDPR);
- ensuring the accuracy of personal data processed (accuracy – Article 5(1)(d) GDPR);
- limitation of personal data retention periods (storage limitation – Article 5(1)(e) GDPR);
- ensuring appropriate security of the personal data (integrity and confidentiality – Article 5(1)(f) GDPR);
- demonstrating compliance with the principles of processing and ensuring the security of personal data (accountability – Article 5(2) GDPR).

6. Data subject's rights

6.1. Each Controller is responsible for ensuring the following data subjects' rights under the GDPR:

- right to withdraw the consent to personal data processing with the subsequent erasure of personal data (Article 7 of the GDPR);
- right to receive of information regarding personal data processed (Article 12-14 of the GDPR);
- right to receive a copy of personal data processed (Article 15 of the GDPR);
- right to rectify of personal data provided if it is incomplete or incorrect (Article 16 of the GDPR);
- right to erase of personal data (Article 17 of the GDPR);
- right to restrict of processing of personal data (Article 18 of the GDPR);
- right to receive personal data provided to us in a structured format and transmit this data to other companies (Article 20 of the GDPR);
- right to object the processing of personal data (Article 21 of the GDPR);
- right to receive information about personal data breach (Article 34 of the GDPR).
- right to lodge a complaint with a supervisory authority, if data subject's rights have been violated (Article 77 of the GDPR).

6.2. The obligations of the Parties on issues related to the processing of data subject' requests are defined in section 7 of this Agreement.

6.3. The Parties are responsible for providing assistance to each other in fulfillment of their obligations to data subjects.

7. Responding to the data subjects' requests

7.1. Each Controller is responsible for processing any data subjects' requests, if the request is related to implementation of data subject's rights or violation of the GDPR provisions, for which the Controller is responsible in accordance with this Agreement.

7.2. If one of the Controllers receives a data subject' request on issues related to the processing of personal data that are the responsibilities of the other Controller, the request must be forwarded to this Controller without undue delay.

7.3. If one of the Controllers receives a request, part of which should be processed by another Controller, this part is immediately forwarded to the Controller for a response. The response to data subject is provided by the Controller who received the corresponding request.

7.4. In connection with forwarding the request or part of the request to another Controller, the data subject must be notified of a possible delay and of the fact of forwarding the request to another Controller.

8. Security processing and demonstrating compliance with the GDPR

8.1. Controllers should develop and agree on appropriate joint policies for the protection of personal data, specifying the minimum set of necessary security measures for the implementation of which each of the Controllers is responsible.

8.2. Taking into account the nature, scope, context and purpose of processing, as well as the risks to the rights and freedoms of data subjects, each Controller must ensure that appropriate technical and organisational measures are taken to ensure the security of the personal data being processed.

8.3. Controllers are jointly responsible for compliance with the requirements of personal data protection in accordance with Article 25 (Data protection by design and by default) of the GDPR.

8.4. Each Controller is responsible for compliance with the requirements for ensuring the security of personal data processing in accordance with Article 32 (Security of processing) of the GDPR.

8.5. Controllers jointly conduct (and document) an assessment of the risks of violation of the rights and freedoms of data subjects. Each Controller implements the necessary measures to reduce the identified risks.

9. The use of Processors and Sub-processors

9.1. Processor – a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

9.2. Sub-processor – a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Processor who was previously appointed by the Controller.

9.3. Controllers have the right to involve Processors in the processing of personal data.

9.4. If the Controller uses Processors, the corresponding Controller must inform other Controllers about it.

9.5. If Processors are involved in the processing of personal data, each Controller is responsible for compliance with the requirements of Article 28 of the GDPR. The Controller must, in particular:

- involve only Processors that provide sufficient technical and organisational security measures in order to meet the requirements of the GDPR and ensure the security of personal data and compliance with the data subjects' rights;
- ensure the conclusion of a Data Processing Agreement between the Controller and the Processor;

- assist the Controller in carrying out a data protection impact assessment if the processing of personal data is likely to result in a high risk to the rights and freedoms of data subjects;
- inform the Controller of cases of violation of applicable legislation in the field of processing and ensuring security of personal data;
- inform the Controller of any anticipated changes in the processing of personal data;
- inform the Controller of the intentions and reasons for the transfer of personal data to third parties and (or) international organisations strictly before the transferring of personal data;
- immediately notify the Controller of the data breach after the Processor became aware of the data breach, with detailed information about the data breach provided in stages as more detailed information is received;
- verify that a valid Data Processing Agreement has been concluded between the Processor and any Sub-processor;
- when a Processor engages a Sub-processor, the Processor must notify the Controllers and agree immediately after they occurred, without undue delay.

9.6. The Parties shall inform each other of the actions taken after the incident is detected and provide a copy of the notification sent to the supervisory authority.

10. Notification about personal data breach

10.1. Each Controller is responsible for compliance with Article 33 (Notification of a personal data breach to the supervisory authority) and Article 34 (Communication of a personal data breach to the data subject) of the GDPR concerning the provision the information about a personal data breach to a supervisory authority and a data subject.

10.2. Where there is any risk to the rights and freedoms of data subjects, the Controller shall notify relevant data protection authorities, without undue delay and, when possible, within 72 hours.

10.3. If a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Controller is obliged to provide the data subject with comprehensive and understandable information about this data breach.

11. Data protection impact assessment and prior consultations

11.1. Each Controller is responsible for compliance with the requirements of the Article 35 (Data protection impact assessment) of the GDPR on carrying out an assessment of impact of the personal data processing to the rights and freedoms of the data subject. If the processing is carried out using new technologies, and taking into account the nature, scope, context and purposes of processing, is likely to result in a high risk to the rights and freedoms of natural persons, Controllers should carry out a data protection impact assessment before processing of personal data.

11.2. Similarly, Controllers are required to comply with the requirements of Article 36 (Prior consultation) of the GDPR when consulting the supervisory authority in advance, whenever possible.

12. Cross-border transfer of personal data

12.1. Controllers may transfer personal data to other countries or international organisations only if necessary and there is an appropriate legal basis.

12.2. Controllers are responsible for complying with the requirements of Chapter V (Transfers of personal data to third countries or international organisations) of the GDPR if personal data is transferred to other countries or international organisations.

13. The Agreement and its termination

13.1. This Agreement shall enter into force when signed by all Parties of the Agreement.

13.2. The Parties can not amend this Agreement. The Agreement is valid for as long as the relevant personal data is processed or until the Agreement is replaced by a new Agreement defining the allocation of responsibilities in connection with processing.

13.3. If one of the Parties violates its obligations, the other Party may terminate this Agreement.

13.4. After the purpose of personal data processing is achieved, the Parties are obliged to choose:

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

14. Responsibility and penalties

14.1 Each Party is responsible to the other party for possible damages in case of violation of the provisions of this Agreement.

14.2 Each Party is responsible to data subjects for possible damage, violation of data subjects' rights when processing personal data under this Agreement.

15. Applicable law

15.1 The Agreement is governed by the laws applicable to the relations of the Parties.

15.2 The parties undertake to comply with the GPDR requirements in the framework of the processes from clause 1.2 above if applicable.

Signatures of the Parties

Party 1	Party 2
Huntflow AM, LLC	[Name of the Controller]
Armenia, YEREVAN, ARABKIR, 36 MANUSHYAN	[Address of the Controller]
Director/ M.Tansky	[Position of authorized person] / [Full name]

Party 3

[Name of the Controller]

[Address of the Controller]

____
[Position of authorized person] / [Full name]

Party 4

[Name of the Controller]
[Address of the Controller]

____
[Position of authorized person] / [Full name]