Data Processing Agreement
Processor

This data processing agreement (the "**DPA**") is executed by and between the Kubeark and the Company (as defined in the signatures block below, each a "**Party**" and together the "**Parties**") on the date the last Party signs in the signatures block below ("**Effective Date**").

Whereas:

(a) the Parties entered into an agreement on or about the Effective Date whereby the Processor will provide certain services (the "**Services**") to the Controller (the "**Main Agreement**");

(b) the Processor may process personal Data (as defined by the Data Protection Laws) on behalf of the Controller in the performance of the Services as stipulated in the Main Agreement (hereinafter, "**Personal Data**");

(c) the Parties wish to lay down the rules and obligations with respect to Personal Data.

Have agreed as follows:

1. Terminology

For the purposes of the DPA, the terminology and definitions as used by Regulation 2016/679 of the European Parliament and of the Council (the "**GDPR**") shall apply. "**Data Protection Law**" means the GDPR and any other law, regulation, ordinance, or legal act which imposes data protection obligations onto a Party. For the purpose of this Agreement Kubeark may be referred to as the "**Processor**" and the Company as the "**Controller**". Further definitions are provided throughout this DPA.

2. Purpose and Applicability

2.1. Kubeark and the Company have concluded this DPA to establish their responsibilities regarding the protection of Personal Data, in accordance with the Data Protection Law. Under this DPA the Company may process Personal Data either as a controller or as a processor, and Kubeark acts as a processor for the Company. This DPA sets forth the general rights and obligations of the Parties, and the specific information and details regarding Personal Data Processing (i.e., purpose, duration, nature and purpose of each processing, type of Personal Data and Data Subjects), as further detailed herein. Any amendment to the processing details described in in this DPA may only be made based on a written instruction from the Company.

2.2. This DPA applies to the Services used by the Company, and solely to the extent that Personal Data is transferred from the Company to Kubeark, as agreed in the Main Agreement and this DPA. Whereas the Company has full control over the Personal Data, it is also responsible to comply with the applicable Data Protection Laws, to assess whether the use of the Services meets its compliance and contractual obligations, and to obtain all permissions, authorizations, and consents for the Processing of Personal Data in accordance with this DPA. This DPA does not apply to:

2.2.1. Personal Data processed through third party cloud integrations, which are subject to their own terms and conditions and privacy policies;

2.2.2. Services that do not entail any transfer of Personal Data from the Company to Kubeark;

2.2.3. Scenarios where the transfer of Personal Data to Kubeark is restricted, such as:

(i) products or services are offered by Kubeark for preview, early access or evaluation;

(ii) where the transfer of Personal Data is subject to certain legal formalities (such as data localization, certification, or registration with the appropriate regulatory bodies, etc.) and such formalities are not yet fulfilled by Kubeark;

(iii) where Personal Data may include protected health information, as regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) ("PHI"), cardholder data ("CHD") and sensitive authentication data ("SAD"), as defined by Payment Card Industry Data Security.

3. Order and Instructions for Processing

3.1. The Company hereby orders Kubeark to process Personal Data on behalf of the Company and

in the performance of the Main Agreement in accordance with this DPA. Kubeark is required to process the Personal Data only subject to, and within, the limits set forth in the documented instructions received in writing from the Company.

3.2. Kubeark will notify the Company without delay if it considers that a Company's instruction or any implementation of an instruction received from the Company breaches or may breach the Data Protection Law. Kubeark will not "sell" the Personal Data within the meaning of the CCPA. To the extent Processing of Personal Data is subject to the CCPA, the Parties agree that Company is the "Business" and Kubeark is the "Service Provider".

3.3. Kubeark will maintain the records of processing for Personal Data required under Article 30(2) of the GDPR and, to the extent applicable to the processing of Personal Data on behalf of Company, make them available to the Company upon request.

4. Confidentiality and Security

4.1. All Personal Data that the Processor receives from the Controller within the context of the DPA is subject to an obligation of confidentiality towards the Controller. The Processor will refrain from using this information for any purpose other than that for which it has acquired it.

4.2. This obligation of confidentiality shall not apply insofar i) the Controller has given consent for the information to be provided to third parties as stipulated in the DPA, or ii) if disclosure of the information to third parties is logically necessary given the nature of the issued assignment and the implementation of the DPA, including without limitation to employees, a contractors, or other sub-processors, or iii) if there is a legal obligation for the Processor to provide the information to a third party, or iv) this right is granted based on the DPA and/or the Main Agreement.

4.3. The Processor shall take all measures at its disposal required to ensure a level of security appropriate to the risk, whilst 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 risks of varying likelihood and severity for the rights and freedoms of natural persons. Notwithstanding, the Company is responsible to safeguard any Personal Data part of its credential information and/or any components under its control, and to assess whether its privacy and security obligations are met when using the Services.

4.4. If The Processor receives any valid request of disclosure of Personal Data from a governmental body, it will: a) make all reasonable efforts to redirect the request to the Controller; b) notify the Controller as soon as possible after receiving a request, unless prohibited by law to send such notification. In such case, Processor will make all lawful efforts to waive such prohibition; c) challenge the legality of such order to disclose if, after a careful assessment, it concludes that there are grounds under the law of the country of destination to do so. If Processor is still compelled to disclose Personal Data, it will disclose only the minimum amount of data necessary to comply with the request of disclosure.

5. Audit

5.1. The Controller may request the Processor to provide information that reasonably demonstrates the Processor's compliance with its obligations under the DPA. The Processor shall provide such information without undue delay.

5.2. To the extent the information provided as per above does not suffice, the Controller may request to perform a verification of the Processor's compliance with its obligations under the DPA, directly or through an independent auditor. The verification shall be performed in accordance with the rules set below:

5.2.1. an audit protocol must be agreed by the Parties and, if applicable, the third-party auditor, with eight (8) weeks in advance of the proposed audit date; the audit plan will describe the scope, duration, third party auditor and start date of the audit and shall be limited as to ensure Kubeark's confidentiality and security obligations towards its employees and counterparties;

5.2.2. if the audit scope described in the audit plan is addressed in a certification or a verification report performed by a qualified third party in the twelve (12) months prior to the Company's audit request, the Company agrees to accept and rely on these reports and Processor's confirmation that there were no material changes in the verified data protection/security measures, and therefore no audit will be performed;

5.2.3. audits may be performed no more than once (1) a year and must be conducted during the business hours, according to Kubeark's policies, and will not interfere with its business activities;

5.2.4. audits may be performed only if a confidentiality agreement is concluded with the Company or the third-party auditor and the audit results will remain confidential and will not be shared with any third party unless agreed by an authorized representative of Kubeark in writing;

5.2.5. unless prohibited by legislation binding on the Parties, the Company must provide Kubeark with a copy of the audit report free of charge;

5.2.6. audits are performed at Company's expense and Kubeark will give reasonable cooperation and assistance.

6. Data Protection Impact Assessment

Upon written request from the Controller, the Processor shall give reasonable assistance to the Controller in carrying out any assessment of the consequences or impact of Processing of Personal Data and in any consultation with the Supervisory Authority, insofar as it relates to the processing of Personal Data under this DPA. Processor will notify the Controller without delay if a Supervision Authority contacts Processor directly with respect to the processing activities that fall within the subject matter of this DPA.

7. Data Subject Rights

7.1. The Controller is primarily responsible for handling and responding to information requests, access requests, rectification requests, erasure requests, restriction of processing requests, and portability requests and the right no to be subject to an automated individual decision making, as made by data subjects (the "**Data Subject Requests**").

7.2. The Processor shall assist the Controller, especially through appropriate technical and organizational measures, insofar as this is possible, with the fulfilment of the Controller's obligation to comply with the Data Subject Requests, in particular with the obligations stipulated above.

7.3. With regard to Data Subject Requests, the Processor shall either i) provide the Controller with the ability to comply with the Data Subject Requests themselves or, ii) if such ability cannot be provided, the Processor shall provide the necessary manual assistance to Controller to comply with the Data Subject Requests.

7.4. Processor shall promptly inform the Controller of requests received by Processor from Data Subjects exercising their rights under the Data Protection Law.

8. Sub-Processors

8.1. The Controller agrees and hereby authorizes the Processor to engage third parties for the processing of the Personal Data (the "**Sub-processors**") and change Sub-processors subject to the rules set our herein. Sub-processors will be subject to the same confidentiality obligations and adequate guarantees for the security of Personal Data as those provided for the Processor in this DPA. The Controller acknowledges, agrees, and hereby gives a written authorization under Article 28 of the GDPR to the Processor to engage its Affiliates as Sub-processors. A list of its Affiliates will be maintained on its website https://kubeark.com/ (or successor page).

8.2. Changes to the Sub-processors will be subject to sending a written notice to the Controller, at the e-mail address available in the Processor's records. Subject to having a legitimate reason under Data Protection Law, Controller will have 30 (thirty) days from the notice to send a written notice to the Processor exercising its right to object to the change and terminate the applicable Service or requesting Kubeark that the Parties discuss in good faith a resolution to the objection no later than the end of the 30-day period. The objection notice will contain at least the following to be valid (i) the name of the Service to be terminated and (ii) the termination date, which will be no later than 30 (thirty) days from the date of the Processor's notice to the Controller. The Company acknowledges its sole and exclusive remedy for objecting to any change in Sub-processors is the termination of the Main Agreement, but only limited to the Service for which the new Sub-processor is intended to be used. After the 30 (thirty) days term with no written notice received from the Controller, Kubeark will deem in

good faith that the Company has accepted the change in Sub-processors.

8.3. Notwithstanding the foregoing rules setting out the procedure for changes in Sub-processors, Processor may replace a Sub-processor without advance notice to Controller where the reason for the change is outside of the Processor's reasonable control and prompt replacement is required for regulatory, security, system integrity, business continuity purposes or other urgent reasons. Processor will inform the Controller of the replacement as soon as possible following such change, and the procedure set out above will apply accordingly.

8.4. **Hosting Location**. Personal Data will be hosted in the region(s) evidenced in the Sub-processor list. Where technically implemented in a particular Service, the Company may configure the hosting location of the Personal Data used therein, provided however that back-ups may have different configurations.

9. International Transfers of Personal Data

9.1. In case of a transfer of Personal Data outside the EU/EEA and/or to a country that is not recognized as providing an adequate level of data protection, the Processor will ensure that (i) standard contractual clauses are in place with respect to such transfer, and (ii) the Processor and the Sub-processor enter into a data processing agreement containing the same or similar provisions as the DPA.

9.2. Processor may transfer Personal Data outside the country in which the Company or its Affiliates using the Services are located, in accordance with this DPA and as permitted under Data Protection Law, and only by offering Transfer Safeguards and ensuring that all transfers are made in accordance with Transfer Safeguards.

9.3. Where Processor is not located in a Third Country and acts as an exporter of Personal Data that is subject to the GDPR or any other law relating to the protection or privacy of individuals that applies in Europe, Processor agrees on SCC with, or relies upon, Transfer Safeguards in connection with, each Sub-processor located in a Third Country that acts as Personal Data importer. Where Processor is located in a Third Country and acts as an importer of Personal Data that is subject to the GDPR or any other law relating to the protection or privacy of individuals that applies in the EEA, to the extent Transfer Safeguards cannot be provided, Processor and Controller, as a Personal Data exporter hereby enter into, and agree that, the SCC shall apply and will be incorporated into this DPA, as follows: a) Module 2 (Controller to Processor) shall apply where Controller is a controller; and b) Module 3 (Processor to Processor) shall apply where Controller is a processor. The description of processing and other details required by the SCC are attached hereinbelow.

9.4. Unless otherwise notified by Processor in writing, if the European Commission amends the SCCs after the Effective Date, the amended SCCs will supersede and replace the SCCs executed between the Parties by virtue of this section. In addition, if and to the extent a court of competent jurisdiction or Supervisory Authority orders (for whatever reason) that the measures described in this DPA cannot be relied on for the purpose of lawfully transferring Personal Data to Third Countries, the Company agrees that Processor may implement any additional measures or safeguards that may be reasonably required to enable a lawful transfer.

10. Personal Data Breach Management

10.1 The Processor shall inform the Controller without undue delay after the confirmation of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed by the Processor for the purpose of this DPA ("**Personal Data Breach**"). The notice will be sent to an e-mail address provided by the Company and available in Processor's records. Upon written request from Controller and without undue delay, the Processor shall provide the necessary information to enable the Controller to document the Personal Data Breach and to notify the Supervisory Authority and the Data Subjects thereof, as required under the Data Protection Law.

10.2 The Processor shall take all measures necessary to restrict the adverse consequences of the

Personal Data Breach and remedy the effects thereof. Unless the context does not allow it, the Processor will do best efforts to consult with the Controller with respect to mitigation measures.

10.3 Parties agree that Processor does not acknowledge any liability or fault by the mere giving notice of a Personal Data Breach. The Company acknowledges that it is responsible for complying with its own legal obligations regarding Personal Data Breach notifications. If the Company suspects that an incident occurred, the Company shall without undue delay notify the Processor at privacy@kubeark.com.

11 Liability

11.1 Each Party is liable for its acts and omissions and obligations set out in this DPA and under the Data Protection Law as applicable to such Party. Processor will remain liable to the Company for the performance of the obligations that its appointed Sub-processors fail to comply with.

11.2 **Limitation of Liability**. Unless otherwise prohibited by applicable laws binding on the Parties, the maximum aggregate liability of each party and/or their affiliates, for any and all breaches and claims (individually and together) under or relating to this DPA, and for all data processing activities contemplated by this DPA, will not exceed the liability cap or monetary limitation set out in the Main Agreement. This limitation applies whether the claim arises from contract, non-conformity or tort and regardless of the theory of liability. Unless otherwise prohibited by applicable laws binding on the Parties, neither Party will be liable to the other for any special, indirect, moral, consequential, incidental, punitive, or exemplary damages, loss of profits, reputation, use, or revenue, or interruption of business, irrespective of whether the other Party has been advised of the possibility of such damage. Processor will not be liable for any damage caused by failure of the Controller to comply with the DPA or any Data Protection Law or policies.

12. Term, Termination, and Retention

12.1. **Term.** This DPA is effective at the Effective Date and will be in force for as long as the Company uses Services under the Main Agreement, without exceeding the duration of the Main Agreement. The Parties may agree to terminate this DPA in writing.

12.2. **Consequences of Termination.** Following termination of the Main Agreement and/or this DPA and upon express written instructions from the Company, Processor will ensure that the Personal Data will be, as requested by the Controller, deleted, or returned to the Processor either manually or, if technically available, via direct export from the relevant Service. In the absence of any written instruction from the Controller given at termination, the Parties agree that this section constitutes notice by the Company to Processor of the instruction to delete the Personal Data within a reasonable time following termination of the Main Agreement, in accordance with the Data Protection Law, unless and to the extent retention is required by applicable law, or the Personal Data has been archived on back-up systems due to the Service functionalities.

13. Other Provisions

13.1. **Entire Agreement.** This DPA constitutes the entire agreement between the Parties with respect to the subject matter hereof and takes prevalence over any prior written or oral agreement between them with respect to such subject matter or in the event of conflicting provisions regarding any rights and obligations granted or incurred by the Parties for purposes of this DPA. Except as otherwise prescribed hereunder, any changes or amendments to the DPA or its Exhibits will be effective only if made in writing and agreed by both Parties. This DPA is without prejudice to the rights and obligations of the Parties under the Main Agreement, which will continue to have full force and effect. This DPA is incorporated into and made a part of the Main Agreement by this reference.

13.2. Provisions from the DPA that are intended by their nature to survive the DPA will remain in full effect after the end of the DPA. Should any of the provisions of the DPA be deemed invalid, unenforceable, or contrary to the law (either in whole or in part), the remaining provisions and/or the valid part of the DPA will be construed as if such invalid or unenforceable provisions were not contained herein. Such illegal, invalid and unenforceable provisions will then be deemed to be replaced by a provision which as closely as possible meets the intention of the Parties when inserting the original provision.

13.3. The DPA is exclusively governed by Romanian law. All disputes arising in connection with the DPA or the performance thereof will be submitted to the Romanian competent court in Bucharest.

The following Annexes are attached after the signatures block:

1. Details of the Personal Data processing.

[SIGNATURE BLOCK FOLLOWS]

Signatures	
Processor: Kubeark SRL	**Controller:**_____
By:	By:
Title:	Title:
Date:	Date:
Authorized Signature:	Authorized Signature:
Address: SKY TOWER Building, 246 Calea Floreasca, 1st floor, 1st District, Bucharest, Romania, tax no. 45781670	Address:

Annex 1
Details of Personal Data Processing

Processor shall process the Personal Data received from the Controller in accordance with the Processing details set out below.

Contact person(s) of the Processor	privacy@kubeark.com
Purpose (reason)	Performance of the Main Agreement
Type	Electronically
Duration	The term of the Main Agreement plus an additional reasonable period after termination until deletion or removal of all Personal Data from the Processor's records, in accordance with the Processor's internal policies and the DPA.
Categories of Personal Data	As determined by the Controller for each Service used under the Main Agreement.
Data Subjects	Individuals whose Personal Data is provided by the Controller to Processor by using the Services.
Data storage/ server location	Location depends on the applicable Service and information is available within each Service or on Processor's website https://kubeark.com/

Annex 2
Details required by the Standard Contractual Clauses and by Annexes I and II

Selection of Module	
Standard Contractual Clauses	Module Two (transfer controller to processor) applies where Company is a Controller. Module Three (transfer processor to processor) applies where Company is a Processor, acting under the instructions of its Controller(s). Module Four (transfer processor to controller) applies where Company is a Controller located in a Third Country, Kubeark is a processor and exports Personal Data back to the Company.

Selection of Options	
Clause 7	The parties wish to adopt Clause 7 Docking which is optional.
Clause 9(a)	Option 2: Processor has Controller's general authorization to engage Sub-processors in accordance with this DPA.
Clause 11(a)	The parties do not wish to adopt the second paragraph of Clause 11(a) which is optional.
Clause 17	Option 1: Member State is Romania.
Clause 18(b)	Member State is Romania.

Annex I – List of Parties		
Data exporter(s)	Identity:	Company, its affiliates and authorised users, as defined under the Main Agreement.
	Contact person's name:	Identified in the Main Agreement.
	Activities relevant to data transferred under these Clauses:	The activities required to perform the Main Agreement: execution of instructions of Company in accordance with the Main Agreement, continuous improvement of service features and functionalities, communication to authorized users, back up, and restoration of Personal Data stored in the Services, security, monitoring etc.
	Role:	Controller or Processor, as applicable
Data importer(s)	Identity:	Kubeark Inc (or one of its affiliates based in a Third Country)
	Contact person's name:	privacy@kubeark.com
	Activities relevant to data transferred under these Clauses:	The activities required to perform the Main Agreement: execution of instructions of the Company in accordance with the Main Agreement, continuous improvement of service features and functionalities, communication to authorized users, back up, and restoration of Personal Data stored in the Services, security, monitoring etc.
	Role:	Processor

Annex I – Description of Transfer	
Annex I – Competent Supervisory Authority	
data subjects whose personal data is transferred	using the Services under the Main Agreement.
The supervisory authority with responsibility for ensuring compliance by the data exporter	The applicable supervisory authority is the authority in the EU Member State where the data exporter is established, or other supervisory authority with the right by operation of law to supervise compliance.
Categories of personal data transferred	Controller determines the categories of data for each Service used under the Main Agreement.
Sensitive data transferred	N/A, performance under the Main Agreement does not require transfer of any sensitive data.
The frequency of the transfer	Personal Data is transferred continuously during the term of the Main Agreement.
Nature of the processing	As necessary for the performance of the Main Agreement.
Purpose(s) of the data transfer and further processing	Performing the Main Agreement. The Personal Data may be related but not limited to the following: a) provide Services which include storage, computer processing, improvement of service, and execution of Company's instructions in accordance with the Main Agreement; b) perform professional services, as agreed under a statement of work; c) solving support tickets raised by the Company in accordance with the Main Agreement, via written tickets, phone calls, basic troubleshooting, or other .
The period for which the personal data will be retained	The term of the Main Agreement plus an additional reasonable period after termination until deletion or removal of all Personal Data from the Processor's records, in accordance with the Processor's internal policies and the DPA.
Transfers to sub-processors	The list of Sub-processors and the processing activities performed by them is made available by Kubeark on the website or during the provision of Services.

Annex II - Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data	
Description of the technical and organisational measures implemented by the data importer(s)	Processor will maintain at least the technical and organizational security measures set out on its website https://kubeark.com/, or otherwise agreed in writing with the Company. Company acknowledges and agrees that such measures are appropriate for the purposes of this DPA. Such measures do not apply if Processor performs Services on the Company's premises and Processor is provided access to Company's systems and data; provided that Processor shall comply with Company's reasonable policies for the protection of Personal Data against unauthorized access.

Annex III - List of Sub-processors

The exporter(s) authorised the use of the following sub-processors:	The list of Sub-processors and the processing activities performed by them is made available by Kubeark on the website or during the provision of Services.

Transfers from other countries	
EU SCC, completed with the details set forth under Section 1 above apply for transfers from the United Kingdom, subject to the following:	
Applicable law	any references to "Directive 95/46/EC" or "Regulation (EU) 2016/679 shall be understood as references to the UK GDPR.
	any references to the "EU", "Union" and "Member State law" shall be understood as references to English law.
Competent authorities	any references to the "competent supervisory authority" and "competent courts" shall be understood as references to the relevant data protection authority and courts in England, unless the EU SCCs as implemented above cannot be used to lawfully Transfer such Data in compliance with the UK GDPR, in which event the UK SCCs will instead be incorporated by reference and form an integral part of this DPA and will apply to such Transfers. Where this is the case, the relevant Annexes or Appendices of the UK SCCs will be populated using the information contained in Section 1 above of this DPA (as applicable).
UK IDTA additional fields	Is personal data received from the Importer combined with personal data collected by the Exporter: No.
	Which Parties may end the UK IDTA: Both Parties.
	Applicable law to the IDTA: England and Wales.
EU SCC, completed with the details set forth under Section 1 above apply for transfers from Switzerland, subject to the following:	
Applicable law	any references to "Directive 95/46/EC" or "Regulation (EU) 2016/679 shall be understood as references to FADP.
Competent authorities	any references to the "competent supervisory authority" shall be understood as reference to "Swiss Federal Data Protection and Information Commissioner (the "FDPIC").
	any references to the competent courts or to any provisions related to contractual claims may be understood as references to the Member State, as set forth under Section 1 subject to data subjects in Switzerland having the possibility to file claims for their rights in Switzerland.